HU 0002181348

(19) Országkód

HU

MAGYAR KÖZTÁRSASÁG

MAGYAR SZABADALMI HIVATAL

SZABADALMI LEÍRÁS

(11) Lajstromszám:

218 134 B

(21) A bejelentés ügyszáma: P 98 01636
(22) A bejelentés napja: 1996. 03. 22.
(30) Elsőbbségi adatok:
08/521,262 1995. 08. 30. US
(86) Nemzetközi bejelentési szám: PCT/US 96/03824
(87) Nemzetközi közzétételi szám: WO 97/08665

(51) Int. Cl.[7]

G 07 F 7/08
G 06 F 17/60

(40) A közzététel napja: 1998. 10. 28.
(45) A megadás meghirdetésének dátuma a Szabadalmi Közlönyben: 2000. 06. 28.

(72) Feltaláló:
Rosen, Sholom S., New York, New York (US)

(73) Szabadalmas:
CITIBANK, N. A., New York, New York (US)

(74) Képviselő:
Szuhai Elemér, DANUBIA Szabadalmi és Védjegy Iroda Kft., Budapest

(54) # Elektronikus kereskedelmi fizetőrendszer és -eljárás, továbbá rendszer, elektronikus kereskedelmi fizetés és átutalási utasítás összekapcsolására

KIVONAT

A találmány elektronikus kereskedelmi fizetőrendszer, amelynek része a vevő (B) ügynöke (2), a vevő ügynökéhez (2) tartozó, vele védett üzenetváltásra alkalmas első pénzmodul (6), a vevő ügynökével (2) első, kódolással védett kapcsolat létesítésére alkalmas szolgáltató (A) ügynöke (4), a szolgáltató ügynökéhez (4) tartozó, vele védett üzenetváltásra alkalmas, az első pénzmodullal (6) második, kódolással védett kapcsolatot létesítő második pénzmodul (6'), amely rendszerben

a vevő ügynöke (2) elektronikus átutalásiutasítás-információt közöl a szolgáltató ügynökével (4), amely információ vételét a szolgáltató ügynöke „kereskedelmi fizetés" jegy (8) adásával visszaigazolja,

a vevő ügynöke (2) a „kereskedelmi fizetés" jegy (8) vétele után elektronikus pénzmegjelenítő első pénzmodulból (6) második pénzmodulba (6') történő kifizetését kezdeményezi.

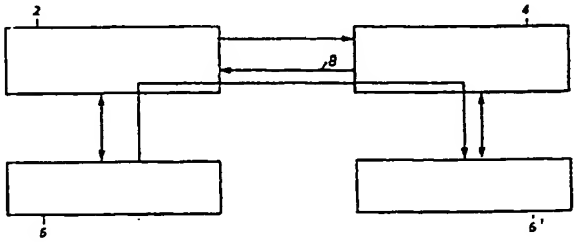
A találmány továbbá elektronikus kereskedelmi fizetőeljárás rendszerben történő alkalmazásra, amely rendszernek része a vevő (B) ügynöke (2), a vevő ügynökéhez (2) tartozó első pénzmodul (6), a szolgáltató (A) ügynöke (4), a szolgáltató ügynökéhez (4) tartozó második pénzmodul (6'), amely eljárás során

a) kódolással védett első kapcsolatot létesítenek a vevő ügynöke (2) és a szolgáltató ügynöke (4) között,

b) a vevő ügynökéből (2) a kódolással védett első kapcsolatban elektronikus átutalásiutasítás-információt közölnek a szolgáltató ügynökével (4),

c) amely információ vételének igazolásaként a szolgáltató ügynökével (4) „kereskedelmi fizetés" jegyet (8) készíttetnek, a „kereskedelmi fizetés" jegybe (8) beleíoglalva, legalább részben, az átutalásiutasítás-információt,

d) a szolgáltató ügynökéből (4) a kódolással védett első kapcsolatban eljuttatják a „kereskedelmi fizetés" jegyet (8) a vevő ügynökéhez (2), amely vevő ügynöke (2) ideiglenesen tárolja a megkapott „kereskedelmi fizetés" jegyet (8),



1. ábra

A leírás terjedelme 56 oldal (ezen belül 39 lap ábra)

HU 218 134 B

e) az első és második pénztármodul (6, 6') között kódolással védett második kapcsolatot létesítenek,

f) amely második kapcsolatban elektronikus pénzt a szolgáltató ügynöke (4) első pénzmoduljából (6) második pénzmodulba (6') juttatnak, amely második pénzmodulban (6) az átutalt elektronikus pénzt ideiglenesen tárolják,

g) az első pénzmodulban (6) a kapcsolat lezárását kezdeményezik, és biztonságosan informálják a vevő ügynökét (2) az elektronikus pénz sikeres vételéről,

h) a második pénzmodulban (6') a kapcsolatot lezárják, a kapcsolat lezárásával az elektronikus pénz tárolásának ideiglenes jellegét véglegesre változtatják, továbbá biztonságosan informálják a szolgáltató ügynökét (4) az elektronikus pénz sikeres vételéről,

i) a vevő ügynökében (2) az első kapcsolatot lezárják, a kapcsolat lezárásával a „kereskedelmi fizetés" jegy (8) tárolásának ideiglenes jellegét véglegesre változtatják,

j) a szolgáltató ügynökében (4) az első kapcsolatot lezárják.

A találmány másrészt rendszer elektronikus kereskedelmi fizetés és átutalási utasítás összekapcsolására távközlőhálózaton, amely rendszernek része egy feltörés ellen védett, első elektronikus tranzakciós eszköz (122), amelynek első processzora van, és egy feltörés ellen védett, az első elektronikus tranzakciós eszközzel (122) biztonságos kapcsolatot tartó első pénzmodul (6), amelynek második processzora van, továbbá része egy feltörés ellen védett, második elektronikus tranzakciós eszköz (122), amelynek harmadik processzora van, és egy feltörés ellen védett, a második elektronikus tranzakciós eszközzel (122) biztonságos kapcsolatot tartó és az első pénzmodullal (6) első, kódolással védett, biztonságos kapcsolat létesítésére alkalmasan kialakított, második pénzmodul (6'), amelynek negyedik processzora van, és amely második tranzakciós eszköz (122) az első tranzakciós eszközzel (122) kódolással védett kapcsolat létesítésére alkalmasan van kialakítva, amely rendszerben

az első processzor elektronikus átutalásiutasítás-információ második elektronikus ügynökkel, az első biztonságos kapcsolatban történő közlésére alkalmasan van kialakítva,

a harmadik processzor a megkapott átutalási információ alapján „kereskedelmi fizetés" jegy (8) készítésére és a jegy (8) első elektronikus ügynökhöz (2) első biztonságos kapcsolatban történő küldésére alkalmasan van kialakítva,

az első processzor a „kereskedelmi fizetés" jegy (8) kiértékelésére és elektronikus pénznek az első pénzmodulból (6) a második modulba (6') történő kifizetésére alkalmasan van kialakítva.

A találmány végül rendszer elektronikus kereskedelmi fizetés és átutalási utasítás összekapcsolására, amely rendszernek része egy feltörés ellen védett, első elektronikus tranzakciós eszköz (122), amelynek első processzora van, és egy feltörés ellen védett, az első elektronikus tranzakciós eszközzel (122) biztonságos kapcsolatot tartó második elektronikus tranzakciós eszköz (122), amelynek második processzora van, amely második tranzakciós eszköz (122) az első tranzakciós eszközzel (122) kódolással védett kapcsolat létesítésére alkalmasan van kialakítva, amelyben

az első processzor elektronikus átutalásiutasítás- és számlalista-információ második elektronikus tranzakciós eszközzel (122) történő közlésére alkalmasan van kialakítva,

a második processzor az átutalásiutasítás-információ számára digitális szignó készítésére és a digitális szignónak „kereskedelmi fizetés" jegybe (8) foglalására alkalmasan van kialakítva,

a második processzor a jegy (8) első elektronikus ügynökhöz (2) első biztonságos kapcsolatban történő küldésére alkalmasan van kialakítva,

az első processzor elektronikus pénznek az első tranzakciós eszközből (122) a második tranzakciós eszközbe (122) harmadik fél közbeavatkozása nélkül történő kifizetésére alkalmasan van kialakítva.

A találmány tárgya elektronikus kereskedelmi fizetőrendszer és -eljárás, továbbá rendszer elektronikus kereskedelmi fizetés és átutalási utasítás összekapcsolására – harmadik fél bevonása nélkül, feltörés ellen védett, elektronikus tranzakciós eszközökkel, védett üzenetváltásra alkalmas kapcsolatban.

Számos különböző elektronikus fizetőrendszer van részben fejlesztés alatt, részben alkalmazásban. Ilyen elektronikus fizetőrendszer van ismertetve jelen bejelentő alábbi, USA szabadalmi leírásaiban: 5453601, 5557518, 5799687. A fenti bejelentések mellékleteiben elektronikus eszközökkel történő fizetésre alkalmas elektronikus pénzrendszer is le van írva, amely eszközök helyettesíthetik a hagyományos készpénzre váltást, készpénzzel, csekkel, bankkártyával történő fizetést és a hagyományos pénzátutalásokat. A rendszerben feltörésnek mechanikusan ellenálló házakba zárt pénzmodulok vannak alkalmazva, amely pénzmodulokban elektronikus pénzmegjelenítő van tárolva. A pénzmodulok alkalmasak azonnali off-line fizetésekre pénzmodulok között [például egy, a vevő zsebében hordott pénzmodul és a szolgáltató (kereskedő) italautomatája között], és alkalmasak hálózaton át történő, on-line fizetésekre is (például hálózaton át beszerzett információért, repülőjegy-, színházjegyfoglalásért stb.).

Az e bejelentésben említett „vevő ügynöke" és „szolgáltató ügynöke" részletesen ismertetve van az US 5557518 számú szabadalmi leírásunkban (benyújtva 1994. április 28-án). Az említett bejelentésben elektronikus vásárlás során elektronikus áruk biztonságos továbbításának eszközei és módjai vannak ismertetve real-time, anonim és pénzlehívási feltételekkel történő fizetés esetén. Az ott ismertetett megoldás lehetővé teszi, hogy

mind a szolgáltató, mind a szolgáltatás vevője biztonságban érezze az érdekeit.

A kereskedelmi fizetéseket többnyire csekkfizetéssel bonyolítják le, de terjed a pénz elektronikus úton történő átutalása (EFT) fizetésmód is. A kereskedelmi fizetésben – akár csekkel, akár elektronikus úton történik – a fizetés során létrejön egy átutalásiutasítás-információ, amely megengedi a fizetés elfogadójának, hogy kezdeményezze a fizető ügyfél kiegyenlítetlen számlájának vagy számláinak pénzlehívással történő kiegyenlítését. Fontos, hogy a kifizetés és az átutalásiutasítás-információ egyezzenek és esetleges vita rendezésében használható bizonyítékul szolgálhassanak mind a kifizető, mind a kifizetést elfogadó számára.

Csekkfizetés esetében az átutalásiutasítás-információ általában a csekkre van nyomtatva. A csekkfizetés azonban költséges mind a fizető, mind a fizetést elfogadó számára. A fizető kiállítja, postázza, kiegyenlíti a csekket, a fizetést fogadó megnyitja a postát, értékeli az információt, és vár arra, hogy a csekket beválthassa. Az ezekkel a műveletekkel kapcsolatos hatékonysági hibák, felmerülő akadályok miatt a felek egyre inkább igénybe vesznek közvetítőket, pénzváltókat.

Az elektronikus fizetésmódok kisebb költséggel járnak mind a fizető, mind a fizetést fogadó fél részére, ezért az elektronikus fizetésmódok (EFT) egyre inkább terjednek. Jelenleg a kereskedelmi fizetéseknek kevesebb mint öt százaléka bonyolódik le elektronikus úton. Az alkalmazott elektronikus fizetések bankrendszeren keresztül történnek. Az ilyen elektronikus fizetésmód alkalmazásának feltétele, hogy mind a fizető, mind a fizetést elfogadó számlavezető bankja, bankrendszere technikailag alkalmas legyen az elektronikus átutalás lebonyolítására, legyen birtokában EFT-eszközöknek. Az EFT-rendszernek alkalmasnak kell lennie arra, hogy a pénz elektronikus átutalásához társítsa az átutalásiutasítás-információt. Az EFT rögzített kapcsolatokat igényel a fizető és a fizetést fogadó bankok között, ami a feleket olyan rendszerbe zárja, amelynek hálózatát bővítése nehezen oldható meg.

Célunk a találmánnyal az ismert elektronikus fizetőrendszerek említett hiányosságainak megszüntetése, olyan elektronikus kereskedelmi fizetőrendszer és -eljárás kialakításával, amellyel a fizetés bank közbeiktatása nélkül lebonyolítható úgy, hogy a fizetés és átutalásiutasítás-információ társítása is megvalósul, továbbá esetleges vita rendezéséhez megfelelő bizonylatokat képez a fizetésről mind a fizető, mind a fizetést elfogadó számára.

A feladat találmány szerinti megoldása elektronikus kereskedelmi fizetőrendszer, amelynek része a vevő ügynöke, a vevő ügynökéhez tartozó, vele védett üzenetváltásra alkalmas első pénzmodul, a vevő ügynökével első kódolással védett kapcsolat létesítésére alkalmas szolgáltató ügynöke, a szolgáltató ügynökéhez tartozó, vele védett üzenetváltásra alkalmas, az első pénzmodullal második kódolással védett kapcsolatot létesítő, második pénzmodul, amely rendszerben

a vevő ügynöke elektronikus átutalásiutasítás-információt közöl a szolgáltató ügynökével, amely információ vételét a szolgáltató ügynöke „kereskedelmi fizetés" jegy adásával visszaigazolja,

a vevő ügynöke a „kereskedelmi fizetés" jegy vétele után elektronikus pénzmegjelenítő első pénzmodulból második pénzmodulba történő kifizetését kezdeményezi.

Előnyösen a szolgáltató ügynöke az átutalásiutasítás-információhoz digitális szignóját fűzi és a digitális szignót belefoglalja a „kereskedelmi fizetés" jegybe.

Célszerűen a vevő ügynöke a „kereskedelmi fizetés" jegy vétele után, mielőtt kezdeményezné az elektronikus pénzmegjelenítő kifizetését, értékeli a digitális szignót.

Előnyösen az átutalásiutasítás-információ tartalmaz egy számlalistát.

A találmány továbbá elektronikus kereskedelmi fizetőeljárás a rendszerben történő alkalmazásra, amely rendszernek része a vevő ügynöke, a vevő ügynökéhez tartozó első pénzmodul, a szolgáltató ügynöke, a szolgáltató ügynökéhez tartozó második pénzmodul, amely eljárás során

a) kódolással védett első kapcsolatot létesítünk a vevő ügynöke és a szolgáltató ügynöke között,

b) a vevő ügynökéből a kódolással védett első kapcsolatban elektronikus átutalásiutasítás-információt közlünk a szolgáltató ügynökével,

c) amely információ vételének igazolásaként a szolgáltató ügynökével „kereskedelmi fizetés" jegyet készíttetünk, a „kereskedelmi fizetés" jegybe belefoglalva, legalább részben, az átutalásiutasítás-információt,

d) a szolgáltató ügynökéből a kódolással védett első kapcsolatban eljuttatjuk a „kereskedelmi fizetés" jegyet vevő ügynökéhez, amely a vevő ügynöke ideiglenesen tárolja a megkapott „kereskedelmi fizetés" jegyet,

e) az első és második pénztármodul között kódolással védett második kapcsolatot létesítünk,

f) amely második kapcsolatban elektronikus pénzt a szolgáltató ügynöke első pénzmoduljából második pénzmodulba juttatunk, amely második pénzmodulban az átutalt elektronikus pénzt ideiglenesen tároljuk,

g) az első pénzmodulban a kapcsolat lezárását kezdeményezzük, és biztonságosan informáljuk a vevő ügynökét az elektronikus pénz sikeres vételéről,

h) a második pénzmodulban a kapcsolatot lezárjuk, a kapcsolat lezárásával az elektronikus pénz tárolásának ideiglenes jellegét véglegesre változtatjuk, továbbá biztonságosan informáljuk a szolgáltató ügynökét az elektronikus pénz sikeres vételéről,

i) a vevő ügynökében az első kapcsolatot lezárjuk, a kapcsolat lezárásával a „kereskedelmi fizetés" jegy tárolásának ideiglenes jellegét véglegesre változtatjuk,

j) a szolgáltató ügynökében az első kapcsolatot lezárjuk.

Előnyösen a szolgáltató ügynökében az átutalásiutasítás-információhoz digitális szignót fűzünk, és a digitális szignót belefoglaljuk a „kereskedelmi fizetés" jegybe.

Célszerűen a vevő ügynökében kiértékeljük a megkapott „kereskedelmi fizetési" jegyet az elektronikus pénz átutalása előtt.

A találmány szerinti megoldás továbbá rendszer elektronikus kereskedelmi fizetés és átutalási utasítás

összekapcsolására távközlőhálózaton, amely rendszernek része egy feltörés ellen védett első elektronikus tranzakciós eszköz, amelynek első processzora van, és egy feltörés ellen védett, az első elektronikus tranzakciós eszközzel biztonságos kapcsolatot tartó első pénzmodul, amelynek második processzora van, továbbá része egy feltörés ellen védett, második elektronikus tranzakciós eszköz, amelynek harmadik processzora van, és egy feltörés ellen védett, a második elektronikus tranzakciós eszközzel biztonságos kapcsolatot tartó és az első pénzmodullal első, kódolással védett, biztonságos kapcsolat létesítésére alkalmasan kialakított második pénzmodul, amelynek negyedik processzora van, és amely második tranzakciós eszköz az első tranzakciós eszközzel kódolással védett kapcsolat létesítésére alkalmasan van kialakítva, amely rendszerben

az első processzor elektronikus átutalásiutasítás-információ második elektronikus ügynökkel, az első biztonságos kapcsolatban történő közlésére alkalmasan van kialakítva,

a harmadik processzor a megkapott átutalási információ alapján „kereskedelmi fizetés" jegy készítésére és a jegy első elektronikus ügynökhöz első biztonságos kapcsolatban történő küldésére alkalmasan van kialakítva,

az első processzor a „kereskedelmi fizetés" jegy kiértékelésére és elektronikus pénznek az első pénzmodulból a második modulba történő kifizetésére alkalmasan van kialakítva.

Előnyösen a harmadik processzor az átutalásiutasítás-információ számára digitális szignó készítésére és a digitális szignónak „kereskedelmi fizetés" jegybe foglalására alkalmasan van kialakítva.

Célszerűen az átutalásiutasítás-információ számlalistát tartalmaz.

Előnyösen a rendszernek a számlalista szerinti számlák összegeinek végösszegét az átutalási utasításban megadott átutalandó összeggel összevető egysége van.

A találmány szerinti megoldás továbbá egy olyan rendszer elektronikus kereskedelmi fizetés és átutalási utasítás összekapcsolására, amely rendszernek része egy feltörés ellen védett, első elektronikus tranzakciós eszköz, amelynek első processzora van, és egy feltörés ellen védett, az első elektronikus tranzakciós eszközzel biztonságos kapcsolatot tartó második elektronikus tranzakciós eszköz, amelynek második processzora van, amely második tranzakciós eszköz az első tranzakciós eszközzel kódolással védett kapcsolat létesítésére alkalmasan van kialakítva, amely rendszerben

az első processzor elektronikus átutalási utasítás és számlalista-információ második elektronikus tranzakciós eszközzel történő közlésére alkalmasan van kialakítva,

a második processzor az átutalásiutasítás-információ számára digitális szignó készítésére és a digitális szignónak „kereskedelmi fizetés" jegybe foglalására alkalmasan van kialakítva,

a második processzor a jegy első elektronikus ügynökhöz, első biztonságos kapcsolatban történő küldésére alkalmasan van kialakítva,

az első processzor elektronikus pénznek az első tranzakciós eszközből a második tranzakciós eszközbe harmadik fél közbeavatkozása nélkül történő kifizetésére alkalmasan van kialakítva.

Előnyösen a „kereskedelmi fizetés" jegy egy számítógépes, bankszámlás kifizetőrendszerben a fizetés bizonylatát képezi.

Célszerűen a rendszernek egy, az átutalási utasítást egy számítógépes, bankszámlás fizetést elfogadó rendszerbe, kifizetetlen számlákkal történő összevetés céljából továbbító második tranzakciós eszköze is van.

Előnyösen az első tranzakciós eszköznek a digitális szignót pénz átutalása előtt értékelő egysége van.

Célszerűen az első tranzakciós eszköznek az elektronikus szolgáltató második tranzakciós eszközéhez társított feltételei érvényességét értékelő egysége van.

Az alábbiakban kiviteli példákra vonatkozó rajz alapján részletesen ismertetjük a találmány lényegét. A rajzon az

1. ábra a vevő és a szolgáltató ügynöke, valamint pénzmoduljaik közötti tranzakciók szemléltető ábrája, a
2A. ábra átutalásiutasítás-információ mezőit szemléltető ábra, a
2B. ábra az átutalásiutasítás-információba foglalt számlalista szerkezetét szemléltető ábra, a
3. ábra „kereskedelmi fizetés" jegy mezőit szemléltető ábra, a
4. ábra tranzakciós eszköz funkciós egységeinek tömbvázlata, az
5A–5D. ábrák megbízott ügynök funkciós egységeinek összetevői, a
6. ábra pénzmodullal fizető kereskedelmi hálózat szerkezete, tömbvázlat, a
7A. ábra sikeres kapcsolat lezárása, protokoll, a
7B. ábra sikertelen kapcsolat megszakítása, protokoll, a
8A–8D. ábrák kereskedelmi pénzmodulos fizetés folyamatábrái, a
9A–9E. ábrák kapcsolatlétesítések, protokoll, a
10. ábra üzenetküldés, protokoll, a
11. ábra fizetési feltételek ellenőrzése, protokoll, a
12. ábra tranzakció visszafejtése, protokoll, a
13A–13E. ábrák fizetések pénzmodullal, protokoll, a
14. ábra üzenetek kódolási rétegeinek szemléltető ábrája, a
15A–15E. ábrák pénzmodulok közötti kapcsolat létesítésének protokollja, a
16. ábra irányított üzenetküldés protokollja, a
17. ábra MM/TA üzenetküldés protokollja, a
18. ábra TA/MM üzenetküldés protokollja, a
19A–19B. ábrák pénzmodulok tranzakciómegszakító protokollja, a
20. ábra E-irányított üzenetküldés protokollja, a
21A–21B. ábra bankjegytranszfer protokoll, a
22. ábra pénzmodulok tranzakciós kapcsolatlezáró protokollja.

Amint az az említett US 5557518 számú leírásunkban ismertetve van egy ügynök (megbízott ügynök) egy eszköz, amelynek hardver- és szoftverrészei vannak. Tokozása ellenáll a feltörési kísérleteknek, és biz-

tonsági protokollok biztosítják a szolgáltatás és a fizetés szimultán és biztonságos lebonyolítását. Az elektronikus pénz előnyösen elektronikus bankjegyek formájában kerül tárolásra, illetve ügynökök közötti mozgatásra. Az elektronikus bankjegy jellege lehet kredit (hitelpénz) és debit (pozitív) pénz. A pénzmodulok is képesek egymással pénzátutaló adatátviteli, kódolással védett kapcsolatot létesíteni. E bejelentés szerinti megoldásban is előnyösen alkalmazhatók az 5453601 számú, 5799087 számú leírás szerinti pénzmodulok.

Hálózaton keresztül történő elektronikus vásárlásnál az áru és a pénz cseréje a vevő és a szolgáltató ügynöke között történik. A kereskedelmi fizetésnél a találmány szerint 2 vevő ügynöke (CTA) 4 szolgáltató ügynökéhez (MTA) átutalásiutasítás-információt küld (1. ábra). Válaszul a 4 szolgáltató ügynöke „kereskedelmi fizetés" 8 jegyet küld a 2 vevő ügynökének. Erre válaszul a vevő 6 pénzmodulja elektronikus pénzösszeget küld át (utal) a szolgáltató 6' pénzmoduljába, a 2 vevő ügynökén (CTA) és a 4 szolgáltató ügynökén (MTA) át.

ÁTUTALÁSIUTASÍTÁS-INFORMÁCIÓ

A vevő számítógépes, bankszámlás kifizetőrendszere átutalásiutasítás-információt készít, amelynek alapján a vevő ügynöke kifizetést eszközölhet. Az átutalásiutasítás-információ a vevő hálózatán át kerül a vevő ügynökéhez. A 2A. ábrán az átutalásiutasítás-információ tartalmának szerkezete van feltüntetve. Az átutalásiutasítás-információ a tranzakció lebonyolításához szükséges információs adatokat tartalmazza, mint például 46 vevőinformáció, 47 szolgáltatóinformáció, így a vevő neve, címe, referenciaszáma, a szolgáltató neve, címe, hálózatának címe, 49 fizetendő összeg, 48 a fizetés napja, 50 számlalista, amelynek példakénti tartalmi szerkezete a 2B. ábrán van feltüntetve. A számlalista a szolgáltató számára a kiegyenlítendő számlák és a fizetett összeg összevetésére és esetleges eltérés rendezésére alkalmas információt tartalmaz, így 51 számlaszámot, 52 megrendelésszámot, 53 az esedékesség napját, 54 a számla összegét, 55 a diszkont összegét, 56 a nettó összeget.

„KERESKEDELMI FIZETÉS" JEGYEK

Az 1. ábra szerinti 2 vevő ügynöke a 2. ábra szerinti „kereskedelmi fizetés" 8 jegyet küld a 4 szolgáltató ügynökének egy tranzakcióban. A „kereskedelmi fizetés" 8 jegy úgy fogható fel, mint az ügynökök tulajdona. A 2 vevő ügynöke csak akkor használhatja a „kereskedelmi fizetés" jegyet, ha a pénztranzakció sikeresen befejeződött.

Amint az az US 5557518 számú szabadalmi leírásban ismertetve van, az ügynökök különböző célra különböző típusú jegyeket állíthatnak ki. A jelen bejelentés vonatkozásában főleg a „kereskedelmi fizetés" jegynek van jelentősége. A „kereskedelmi fizetés" jegy azonosítja a kereskedelmi fizetés részletes jellemzőit, és tartalmazza a fizetést elfogadó digitális szignóját, és a vevő használhatja azt vita esetén bizonylatként.

A 3. ábrán egy „kereskedelmi fizetés" 8 jegy egy lehetséges kialakítása van szemléltetve. A „kereskedelmi fizetés" 8 jegynek például hat szekciója van: 10 azonosító, igazolt 12 komponensek, 14 jegykibocsátó szignója, 16 kibocsátó bizonylata, 18 jegytranszferlista és 20 küldő szignók. Az egyes szekciók is különböző mezőkből állnak.

A 10 azonosító szekció például az alábbi mezőkből tevődik össze: 22 szolgáltató vagy hatóság, amely mezőben a jegyet kiállító szolgáltató vagy hatóság azonosítója (például a pénzlehívási, illetve működési feltételekből kimásolt neve) van feltüntetve, továbbá tartalmazza a feltételek lejártának dátumát is. Egy 24 vevő ügynöke adatai mező tartalmazza a jegyet elfogadó ügynök azonosító számát és az ügynök meghatalmazásának lejárati dátumát is. Egy 26 jegytípusmezőben van megjelölve a jegy típusa (például kredit- vagy debitkártya, „kereskedelmi fizetési" jegy, „kereskedelmi fizetés" jegy stb.).

A 12 komponensek szekció a jegy törzsét képező, a jegy típusától és alkalmazási céljától függően különböző adatokat tartalmaz. A 3. ábrán példák vannak bemutatva a 12 komponensek szekció tartalmára.

Ha a jegy egy „kereskedelmi fizetés" jegy, akkor a 12 komponensek szekció például tartalmazhat egy 36 vevőinformáció-mezőt, egy 38 szolgáltatóinformáció-mezőt, egy 40 fizetés dátuma mezőt, egy 42 fizetendő összeg mezőt, és egy 44 átutalásiutasítás-információ szignója mezőt, amely a szolgáltató ügynökének digitális szignója az átutalásiutasítás-információn.

A 14 jegykibocsátó szignója szekció a jegy készítőjének a 10 azonosítóhoz és 12 komponensekhez fűzött digitális szignóját tartalmazza. Ilyen digitális szignó a kibocsátó megbízott ügynökének egyéni kulcsával készül.

A 16 kibocsátó bizonylata szekció egy harmadik fél, a megbízott ügynökség által kiállított bizonylat a kibocsátó digitális szignójával, amely szignó igazolja a kibocsátott „kereskedelmi fizetés" 8 jegy autentikusságát. Az ilyen bizonylat a kibocsátó megbízott ügynöke tulajdonának tekinthető. A bizonylatok és digitális szignók alkalmazása ismert, és le van írva például D. W. Davies and W–L. Price, Security For Computer Networks (John Wiley & Sons, 1984) irodalmi helyen.

A 18 jegytranszferlista szekció a jegy ügynökök közötti transzfereivel kapcsolatos információkat tartalmaz a kibocsátástól kezdve sorrendben. A 18 jegytranszferlista például az alábbi mezőket tartalmazza: 28 elfogadó ügynök azonosító kód, 30 küldő ügynök azonosító kód, 32 küldő ügynök bizonylata, 34 jegytranszfer dátum/idő mező. A 18 jegytranszferlista feljegyzést tartalmaz a jegy mindegyik tranzakciójáról, így leírja a jegy történetét (múltját). Megjegyzendő, hogy az ügynökök azonosítójának a 28 elfogadó ügynök azonosító kód mezőben egyeznie kell a 30 küldő ügynök azonosító mezőben előző feljegyzés szerinti azonosítóval. Valahányszor a „kereskedelmi fizetés" 8 jegy transzferálva van ügynökök között, a küldő mindannyiszor szignálja a jegyet a megelőző öt szekciót átfogóan, erre a küldő ügynök egyedi kulcsát alkalmazva.

A 20 küldő szignók szekció minden tranzakciónál frissítve van a legújabb digitális szignóval, így a küldők szignóiból egy lista képződik.

TRANZAKCIÓS ESZKÖZÖK

A 4. ábrán egy 122 tranzakciós eszköz tömbvázlata van feltüntetve. A 122 tranzakciós eszköz lehet például a vevő tranzakciós eszköze, vagy a szolgáltató (eladó)

tranzakciós eszköze, mindkét célra hasonló felépítésű 122 tranzakciós eszköz használható. A 122 tranzakciós eszköz három egységből tevődik össze: 124 gazdaprocesszorból, 120 ügynökből (megbízott ügynök feladatát ellátó egység) és 6 pénzmodulból. A 122 tranzakciós eszköz egységei közötti kapcsolat ellátására például 126 busz szolgál. A 2 vevő ügynöke (CTA) a vevő (B) tranzakciós eszközének (CTD) része, a 4 szolgáltató ügynöke a szolgáltató (A) tranzakciós eszközének (MTD) része.

A 4. ábrán a 124 gazdaprocesszor funkcionális egységei fel vannak tüntetve. Ezek az alábbiak: 128 kapcsolatok, 130 tranzakcióalkalmazások, 132 humán/gépi interfész, 136 dátum/idő, 134 üzenetmenedzser.

A 128 kapcsolatok funkciós egység a 122 tranzakciós eszköz külső kapcsolatait támogatja. A külső kapcsolatok lehetnek vezetékes vagy vezeték nélküli, széles sávú vagy keskeny sávú, kompatibilis kapcsolatok eszközök között. A 128 kapcsolatok funkció létesít kapcsolatot két 122 tranzakciós eszköz között, vagy egy hálózattal a hálózaton át közvetett kapcsolatot létesít más 122 tranzakciós eszközzel vagy ügynökszerverrel.

A 130 tranzakciós alkalmazások funkció számos feladatot lát el. Így például kifizethet elektronikus pénzzel lebonyolítandó tranzakció előtt keletkezett számlákat. Általában az mondható, hogy a 122 tranzakciós eszköz tartalmaz minden olyan eljárási eszközt, ami elektronikus tárgy, elektronikus pénz, feltételek vagy más 8 jegyek kiválasztásához, megvásárlásához és esetleg használatához, illetve eladásához szükséges.

A 132 humán/gépi interfész útján tart kapcsolatot a tulajdonos a 122 tranzakciós eszközével, ezt látja és érzékeli. A 132 humán/gépi interfészt alkothatja billentyűzet, egér, ceruza, hang, érzékeny ernyő, ikonok, menük stb. A 132 humán/gépi interfész a 122 tranzakciós eszköz egységeivel van a 134 üzenetmenedzser közvetítésével kapcsolatban. Számos alkalmazásban elhagyható a 132 humán/gépi interfész: teljesen automatizált tranzakciós eszközök esetében.

A 136 dátum/idő funkció óráját a tulajdonos állítja be. Az általa szolgáltatott adatok, például az aktuális dátum, időpont és időzóna. A dátum/idő információt a funkció mindannyiszor megadja a 120 ügynök számára, amikor azt használatra megnyitották.

A 134 üzenetmenedzser vezérli a 122 tranzakciós eszközön belüli kapcsolatokat: így a 124 gazdaprocesszor, a 120 ügynök és a 6 pénzmodul közötti kapcsolattartást.

ÜGYNÖKÖK

Az 5A. ábrán a 120 ügynök funkcionális egységei vannak tömbvázlatszerűen szemléltetve. Az elektronikus kereskedelmi fizetőrendszerben háromféle 120 ügynököt alkalmazunk, amelyek néhány sajátos 146 átutalófunkcióban eltérnek egymástól. Az 5B. ábrán a 2 vevő ügynökében (CTA) alkalmazott 146 átutalófunkció, az 5C. ábrán a 4 szolgáltató ügynökében (MTA) alkalmazott 146 átutalófunkció, az 5D. ábrán hatóság tranzakciós eszközébe (ATD) ágyazott ügynök 146 átutalófunkciói vannak szemléltetve. Hatóság tranzakciós eszköze (ATD) például kártyakibocsátó és a pénzlehívási feltételeket ellenőrző, feltételes fizetést engedélyező banknál kerül alkalmazásra.

Az 5A. ábrán feltüntetett 120 ügynök 138 külső interfész funkciója fizikai kapcsolatot létesít a 124 gazdaprocesszorral és a 6 pénzmodullal, amelyek a 122 tranzakciós egységbe vannak beágyazva. Egy 140 üzenetinterfész funkció kidolgozza és irányítja az ügynökön belüli és az ügynökök közötti üzeneteket. Egy 142 kapcsolatmenedzser létesíti és megszakítja, illetve lezárja az ügynökök közti és az ügynök-ügynök szerver közti kapcsolatokat. Egy 144 biztonsági menedzser fenntartja a biztonsági információkat (mint például az ügynökök bizonylata és a megbízhatatlanok listája), továbbá biztonságos kapcsolatot létesít a másik üzletfél ügynökével (a 124 gazdaprocesszor útján) és a saját ügynök 6 pénzmoduljával. Egy 146 átutalófunkció a tranzakció lebonyolításához szükséges protokollokat tartalmazza. Ezek különbözőek lehetnek aszerint, hogy a vevő ügynökéé (CTA), a szolgáltató ügynökéé (MTA) vagy a hatóság ügynökéé (ATA) a 146 átutalófunkció.

Az 5B. ábrán a vevő ügynökének 146 átutalófunkcióját részletező példa van feltüntetve. Egy 158 vásárlásfunkció 8 jegyért vagy elektronikus árukért történő kifizetést valósít meg. Egy 160 gazdához funkció egy interfészt képez a 124 gazdaprocesszor felé. Egy 164 jegyet bemutat funkció információ vagy szolgáltatás elnyerése érdekében a 8 jegy bemutatásáról gondoskodik. Egy 166 feltételeket lekér funkció a pénzlehívási feltételeket tartalmazó jegy vételében működik közre. Egy 162 tranzakció log funkció feljegyzéseket tárol az ügynök tranzakcióiról. Mind a 2 vevő ügynöke, mind a 4 szolgáltató ügynöke készít tranzakciófeljegyzéseket, amelyek az alábbi adatokat tartalmazzák: a tranzakció típusa (például a jegy típusú), a jegy tranzakció előtti alakja, vitainformáció a vita dátumával (amit mindegyik ügynök használ a vita dialógusában), állapot, szolgáltató döntése (például kicserél, visszaszolgáltat, megtagad) és bizonylatfrissítő információk (például az újrabizonylatolás dátuma). Egy 168 „párbeszédet kezdeményez" funkció mutatja be az elektronikus árut, ha a vevő elégedetlen vele.

Az 5C. ábrán szolgáltatói 146 átutalófunkció összetétele van szemléltetve. Egy 170 vásárlásfunkció 8 jegyet, illetve elektronikus árukat cserél fizetéssel. Egy 172 gazdához funkció egy interfész a tranzakciós eszköz 124 gazdaprocesszora felé. Egy 176 jegyet átvesz funkció feldolgozza az átvett jegyet a szolgáltatásnyújtás vagy információszolgáltatás érdekében. Egy 177 feltételeket lekér funkció lekéri a szolgáltató feltételeit. Egy 174 tranzakció log funkció tárolja az ügynök tranzakcióiról készült feljegyzéseket. Egy 178 vitamegoldó funkció veszi a 8 jegyet és az elektronikus tárgyat (árut) a vevő kifogásai okának megszüntetése érdekében.

Az 5D. ábrán hatósági 146 átutalófunkció összetétele van szemléltetve. Egy 180 „feltételeket készít" funkció állítja össze és szállítja a pénzlehívási feltételeket kérőnek a feltételeket tartalmazó kártyát, illetve kártyaadatokat. Egy 182 gazdához funkció: interfész a tranzakciós eszköz 124 gazdaprocesszora felé. Egy 184 jegyet átvesz funkció feldolgozza az átvett 8 jegyet a szolgálta-

tásnyújtás vagy információszolgáltatás érdekében. Egy 186 feltételeket megújít funkció elfogadja az eddigi feltételeket, és azokat újra kibocsátja új lejárati dátummal ellátva. Egy 183 tranzakció log funkció tárolja az ügynök tranzakcióiról készült feljegyzéseket. Egy 185 feltételeket lekér funkció megszerez hatósági feltételeket.

Az 5A. ábra szerinti 150 pénzmodulhoz funkció egy interfész a saját tranzakciós eszköz 6 pénzmodulja felé, amelyen át fizetési utasítás adható. Egy 152 rejtjelezés funkció közös kulccsal és szimmetrikus kulccsal rejtjelező funkciókat lát el. Bármely ismert rejtjelező eljárás alkalmazható, így például az ismert RSA- és DES-eljárások is. Egy 148 jegytartó funkció készít „kereskedelmi fizetési" 8 jegyet a 4 szolgáltató ügynökében, vagy tárol és előhív 8 jegyet, a 2 vevő ügynökében. Egy 156 véletlenszám-generátor véletlen számokat generál a rejtjelező kulcsok előállításához. Egy 154 dátum/idő funkció a gazdaprocesszor által szállított dátum- és időadatokkal megdátumozza a 8 jegyet és értékeli a bizonylatokat, bemutatott jegyeket. A pillanatnyi órainformációt betápláljuk a 120 ügynökbe minden alkalommal, amikor tranzakció céljából megnyitjuk (bekapcsoljuk és bejelentkezünk). A 120 ügynök az információt kikapcsolásáig tartja meg.

Az ügynök/pénzmodul hardver állhat például az alábbiakból: egy, a tranzakciós protokollokat lefuttató mikrovezérlő (például az INTEL 196 családból), egy nagy sebességű felejtő memória (SRAM), az operációs rendszernek, az alkalmazási rutinok egy részének, a rejtjelezési adatoknak a műveletvégzések idején történő tárolására, egy nem felejtő memória az operációs rendszer, az alkalmazási szoftverek, jegyek, elektronikus pénz, transzferfeljegyzések és más adatok állandó tárolására, egy integrált áramkörös óra, amely referenciaidő-adatot szolgáltat, akkumulátor az óra számára, zajdióda vagy más véletlen jelforrás a véletlenszám-generátor számára.

RENDSZERÁTTEKINTÉS

A 6. ábrán elektronikus kereskedelmi fizetőrendszer példakénti felépítése van szemléltetve. 188 vevő tranzakciós eszköze a 198 szolgáltató tranzakciós eszközével előnyösen 191 vevőhálózatán, 190 bekötőhálózaton és szolgáltatói 192 hálózaton át tarthat kapcsolatot. A vevő számítógépes, bankszámlás kifizetőrendszere elkészíti az átutalásiutasítás-információt a számlalistával együtt, és megküldi azt a 188 vevő tranzakciós eszközének.

A 188 vevő tranzakciós eszköze az átutalásiutasítás-információ birtokában ellenőrzi, van-e elegendő tárolt pénze a kifizetés teljesítéséhez, szükség esetén azt is, képes-e másik tranzakciós eszközből vagy bankszámláról (lásd bővebben az US 5453601 számú leírást) kiegészíteni pénzkészletét. Ha a fizetés kreditpénzzel történik, ehhez a 188 vevő tranzakciós eszközének vagy megnyitott hitelkerettel kell rendelkeznie, vagy bankhoz kell fordulnia hitelkeretért.

Ha a 188 vevő tranzakciós eszköze rendelkezik egyrészt az átutalásiutasítás-információval, másrészt a kifizetés teljesítéséhez szükséges pénzeszközzel, akkor kapcsolatba léphet a 192 szolgáltatói hálózattal a saját 191 vevőhálózatán és 190 bekötőhálózaton keresztül. A 192 szolgáltatói hálózat biztosít kapcsolatot a 198 szolgáltatói tranzakciós eszközzel (MTD) és a szolgáltató számítógépes, bankszámlás 193 fizetést elfogadó rendszerével, amely 193 fizetést elfogadó rendszer összehasonlítja a könyvelés kiegyenlítetlen számlaadatait a vett átutalásiutasítás-információval. A találmány szerinti elektronikus fizetőrendszerben ezután a vevő elektronikus pénz pénzmodulok közötti átutalásával biztonságosan teljesítheti fizetési kötelezettségét, amire válaszként visszakapja az átutalásiutasítás-információt a szolgáltató tranzakciós eszközének digitális szignójával ellátva.

FOLYAMATÁBRÁK

A további ábrákon feltüntetett folyamatábrákon A és B általában a vevőre és szolgáltatóra, illetve 122 tranzakciós eszközükre utaló jelölés az egymással kapcsolatot létesítő tranzakciós eszközök fő részeinek (120 ügynök, 124 gazdaprocesszor, 6, 6' pénzmodul) és funkciós egységeinek azonosításában. „A biztonsági menedzser" például A tranzakciós eszközének és ezen belüli 120 ügynökenek a 144 biztonsági menedzser funkciós egységét (5A. ábra) jelöli.

A folyamatábrák némelyik kockája egy-egy szubrutin lefuttatását fedi, az A 122 tranzakciós eszközében futó, de nem csak ahhoz kötött szubrutint és funkciós egységeit X jelöléssel, a B 122 tranzakciós eszközében futó szubrutint és funkciós egységeit Y jelöléssel láttuk el. Így például „kapcsolat létesítése XΨY" a folyamatábrában egy szubrutin lefuttatását jelenti. Az ezzel előhívott szubrutin folyamatábrájában X=A, Y=B értendő.

KAPCSOLAT MEGSZAKÍTÁSA, LEZÁRÁSA

A vevő ügynöke és a szolgáltató ügynöke (együttműködő ügynökök) közötti kapcsolatban 8 jegy és elektronikus pénz cserélnek gazdát. Ezeket a tranzakciókat biztonságosan kell lebonyolítani, hogy egyik oldalon se keletkezhessen vagy maradhasson fenn többlet. Így nem engedhető meg, hogy az elektronikus pénz vagy jegy duplikálódjék, így a tranzakciók végén valamiből kétszer annyi legyen, mint a tranzakciók megkezdése előtt. Ugyanígy megengedhetetlen elektronikus pénz vagy jegy elvesztése a tranzakció megszakadása esetén. Ha például a kölcsönös tranzakció kezdetén A-nak van egy 8 jegye, amit átküld B-nek, az szükséges, hogy a tranzakció végén a 8 jegy B-nél legyen, és A-nak ne legyen meg ez a 8 jegye. Különben előfordulhatna az, hogy a tranzakció végén A is, B is birtokol egy ilyen jegyet (jegy duplikálása), vagy előfordulhatna az is, hogy sem A, sem B nem lenne a 8 jegy birtokában (jegy elvesztése).

Annak érdekében, hogy a duplikálás vagy elvesztés valószínűségét a minimumra szorítsuk le, tranzakciófeljegyzéseket szükséges készíteni, annak a lehetőségnek a figyelembevételével, hogy természetes, véletlen okból vagy szándékosan a tranzakció lezárása előtt megszakadhat a kapcsolat. Ilyen természetes ok lehet például, ha megszakad az adatátviteli vonal, amelyen a kapcsolat folyamatban van. A duplikáció vagy elvesztés lehetőségének leszorítása elérhető oly módon, hogy azt az időablakot, amelyben ilyen esemény bekövetkezhet,

minél kisebbre alakítjuk. A szándékos megszakító beavatkozás lehetőségének csökkentése érdekében csökkenteni szükséges az ilyen beavatkozáshoz fűződő érdekeket, hogy ne érje meg megkísérelni a beavatkozást. Ha például egy beavatkozó csak veszíthet, például elveszíti a jegyét vagy pénzét, akkor nem éri meg neki beavatkozni a tranzakciós folyamatba.

Ezek a koncepciók érvényesülnek a találmány szerinti elektronikus pénzterjesztő rendszerben és eljárásban, az alkalmazott protokollokban. Ezt annak megvalósításával értük el, hogy az ügynökök, illetve pénzmodulok kapcsolatában a megszakítást vagy lezárást mindig konzekvensen, szimmetrikusan alkalmazzuk. Ha például A a tranzakció (sikeres) lezárását választja, akkor B oldalán is automatikusan lezárás történik, ha viszont A egy tranzakció megszakítását választja, akkor automatikusan megszakítás történik B oldalán is. Egy inkonzisztencia fellépésekor a konzisztencia elérése és a duplikáció vagy elvesztés valószínűségének minimumra csökkentése érdekében a tranzakcióprotokollok időhatárt szabnak a tranzakció sikeres befejezhetőségének.

A 7A. ábrán kapcsolat lezárása (sikeres tranzakció), a 7B. ábrán kapcsolat megszakítása (sikertelen tranzakció) protokolljának folyamatábrája van feltüntetve.

A megszakítás szubrutin (7B. ábra) az adott 120 ügynökön belül fut le a tranzakció során bekövetkezett valamilyen hiba esetén. A megszakítás szubrutin lefutása visszafejti az addigi lépéseket, és visszaállítja a tranzakció megkezdése előtti állapotot a 120 ügynökben. A szolgáltató 120 ügynöke, ha a megszakítás akkor történik, amikor a pénzlehívás már engedélyezve van a 208 engedélyező hálózat által, az engedélyt is visszavonatja.

Kapcsolat lezárása szubrutin az adott ügynökön belül fut le, ha a tranzakció sikeresen befejeződött. Ekkor a 120 ügynök feljegyzést készít a sikeres tranzakcióról a tranzakció log-jában történő megőrzésre, és ezután készen áll újabb tranzakcióra. Ha például egy jegytranszfer során a szolgáltató A ügynöke elektronikus 8 jegyet készít és ad át a vevő B ügynökének, és ez a kapcsolat megszakítása nélkül sikerült, A ideiglenesen tartja meg a 8 jegyet. Amikor A és B lezárják a kapcsolatot, ezzel a jegy birtoklása elveszti feltételes jellegét, és véglegessé válik. Ha viszont A és B nem lezárják, hanem megszakítják a kapcsolatot, akkor A-nál megmarad a 8 jegy, amelynek másolatát átküldte, és B-nél a lépések visszafejtése során törlődik az ideiglenesen tárolt 8 jegy. A törlésnek számos ismert módja van.

Hasonló a helyzet a 6, 6' pénzmodulok kapcsolatában, amelyben elektronikus pénz átutalása történik. Elektronikus pénz vásárlása során elektronikus pénz (elektronikus bankjegyek formájában) vándorol A pénzmodulból B pénzmodulba. Ennek során A pénzmodul a pénzállományából ideiglenesen levonja az átutalt összeget, B pénzmodul pedig ideiglenesen tárolja az átutalt összeget. Ha mindkét – A és B – pénzmodul lezárja a kapcsolatot, akkor a levonása és B pénz tárolása elveszti feltételes jellegét, és véglegessé válik.

A 7A. ábra szerinti „kapcsolat lezárása" szubrutin az alábbi lépéseket foglalja magában: A gazdához: tranzakció log frissítése (230 lépés), „tranzakció befejezve" üzenet (232 lépés), A kapcsolatmenedzser: megjegyzi: a tranzakció befejezve (234 lépés).

A 7B. ábra szerinti „kapcsolat megszakítása" szubrutin az alábbi lépéseket foglalja magában: A kapcsolatmenedzser visszafejti a lépéseket, és megjegyzi az ügynökök közötti kapcsolat megszakadását (236 lépés), A gazdához funkció: üzenet gazdának: tranzakció megszakadt (238 lépés).

A kapcsolatmegszakító szubrutin közvetlenül, automatikusan beindul, ha például a 120 ügynök megállapítja, hogy egy bizonylat nincs érvényben. Beindítható a megszakító szubrutin akkor is, ha egy várt akció nem következik be. Ha például két 120 ügynök egymással kapcsolatban áll, mindketten figyelik az idő múlását egy időzítőprotokoll futtatásával. Például ha egy első 120 ügynök üzenetet küldött a vele kapcsolatban lévő másik 120 ügynöknek, és arra választ vár az első 120 ügynök A kapcsolatmenedzsere beállít egy időzítőt, és az időzítő lefutásakor megszakít. Az A kapcsolatmenedzser sorszámozhatja is az elküldött üzeneteket, amely sorszám megjelenik a másik B 120 ügynök válaszüzenetében.

Ha az időzítés lefut, mielőtt a válaszüzenet megérkezett volna, az A kapcsolatmenedzser rákérdez B kapcsolatmenedzsernél, hogy a tranzakció folyamatban van-e még B-ben. Ha B nem válaszol, akkor A kapcsolatmenedzser megszakítja a tranzakciót. Ha A kapcsolatmenedzser azt a választ kapja, hogy a tranzakció B-ben még folyamatban van, akkor az időzítőjét későbbi időpontra állítja be. Ha A kapcsolatmenedzser egymás után, meghatározott számú alkalommal azt a választ kapja, hogy a tranzakció B-ben még folyamatban van, anélkül, hogy a várt válaszüzenet megérkezne, akkor megszakítja a tranzakciót. A 6, 6' pénzmodulok közötti kapcsolatban ehhez hasonló időzítési rendszer érvényesül.

KERESKEDELMI FIZETÉS PÉNZMODULLAL

A 8A–8D. ábrákon pénzmodulok közötti kereskedelmi fizetés folyamatábrái vannak feltüntetve. Indításként a kifizető (vevő) számítógépes, bankszámlás 189 kifizetőrendszere átutalásiutasítás-információt készít és juttat el A gazda tranzakciós alkalmazás funkcióhoz (HTA). Bár a 189 kifizetőrendszer előnyösen egy automatizált rendszer, a jelen találmány tanításai kézi vezérlésű rendszerre is (ahol az adatok beadása bebillentyűzéssel történik) alkalmazhatók. A gazda tranzakciós alkalmazás funkció (HTA) összeköttetést létesít B gazda tranzakciós alkalmazással (HTB), előnyösen a 191 vevő hálózatán, 190 bekötőhálózaton és 192 szolgáltatói hálózaton át (700 lépés), és A vevő kereskedelmi fizetés működésmódot választ. A gazda tranzakciós alkalmazás funkció (HTA) üzenetet küld A ügynöknek, hogy fizessen az elektronikus kereskedelmi fizetőrendszerben (702 lépés), B gazda tranzakciós alkalmazás funkció (HTB) üzenetet küld B ügynöknek, hogy fogadja a kereskedelmi fizetést (704 lépés).

Biztonságosan védett kapcsolat létesítése (706 lépés).

A 9. (9A–9E.) ábra szerinti szubrutinban (részletezve az US 5557518 számú szabadalmi leírásunkban kapcsolat létesítésekor A kapcsolatmenedzser A ügynök (ATA) bizonylatát kéri (296 lépés), A biztonsági mene-

dzser az ügynök bizonylatát átküldi B kapcsolatmenedzsernek (298 lépés), A kapcsolatmenedzser A bizonylatát megküldi B ügynök kapcsolatmenedzserének (300 lépés). B kapcsolatmenedzser veszi a bizonylatot (302 lépés), B biztonsági menedzser átveszi a bizonylatot B kapcsolatmenedzsertől (304 lépés).

A B ügynökének közös kulcsfunkciója értékeli A ügynök bizonylatának érvényességét (306 lépés) az US 5557518 és US 5799087 számú leírásunk szerinti protokollal. 308 lépés: A ügynök A-tól kapott bizonylata érvényes? Ha A ügynök bizonylata nem érvényes, akkor B kapcsolatmenedzser ezt megjegyzi, és üzenetet küld A kapcsolatmenedzsernek: a kapcsolat megszakad (310 lépés). A kapcsolatmenedzser ezt megjegyzi (312 lépés). Ha A ügynök bizonylata érvényes, akkor B biztonsági menedzser ellenőrzi, nincs-e A ügynök a megbízhatatlanok listáján (314 lépés). 316 lépés: A ügynök a megbízhatatlanok listáján van? Ha A ügynök a megbízhatatlanok listáján van, a kapcsolat a 310–312 lépések szerint megszakad.

Ha A ügynök nincs a megbízhatatlanok listáján, akkor B véletlenszám-generátora R(B) véletlen számot és B értékelő üzenetet (ami egy másik véletlen szám) generál (318 lépés). Az R(B) véletlen szám egy esetleg használandó kapcsolatkulcs alapját képezi. A B értékelő üzenet is egy véletlen szám, amely az üzenet ismétlésének megakadályozását szolgálja. A B biztonsági menedzser összegyűjti az R(B) véletlen számot, a B értékelő üzenetet és A bizonylatát egy, az A ügynöknek küldendő üzenetbe (320 lépés). B közös kulcsfunkciója ezt az üzenetet kódolással titkosítja kódoláshoz A ügynök közös kulcsát (TA/PK) használva, amely közös kulcsot B ügynök az A ügynök bizonylatával együtt kapott meg (322 lépés). B kapcsolatmenedzser a kódolt üzenetet A kapcsolatmenedzserhez küldi (324 lépés). A kapcsolatmenedzser veszi az üzenetet B kapcsolatmenedzsertől (326 lépés).

A közös kulcsfunkció dekódolja az üzenetet a saját (közös kulcsának megfelelő) egyéni kulcsát használva (328 lépés), és értékeli az A bizonylat egyezését az eredetivel, tehát az érvényességét (330 lépés). Ha A ügynök visszakapott bizonylata nem érvényes, akkor az A kapcsolatmenedzser ezt megjegyzi, és tranzakció megszakítóüzenetet küld B kapcsolatmenedzsernek (332 lépés). B kapcsolatmenedzser veszi az üzenetet, és megjegyzi, hogy a kapcsolat megszakadt (334 lépés). Ha A bizonylata érvényes, akkor A biztonsági menedzser ellenőrzi, nincs-e B ügynök a megbízhatatlanok listáján (336 lépés). 338 lépés: B ügynök a megbízhatatlanok listáján van? Ha B ügynök a listán van, akkor a kapcsolat a 332–334 lépésekben megszakad.

Ha B ügynök nincs a megbízhatatlanok listáján, akkor A véletlenszám-generátor R(A) véletlen számot és A értékelő üzenetet generál (340 lépés), A dátum/idő funkció dátum/idő adatot küld A biztonsági szervernek (342 lépés). A dátum és idő adatokat A és B kicserélik egymás között, hogy esetleg feljegyezhessék a tranzakció log-jukban. A biztonsági menedzser ezután formál és tárol egy ügynökök közötti TATA=R(A)xorR(B) kapcsolatkulcsot (344 lépés). A TATA kapcsolatkulcsot a két 120 ügynök közötti kapcsolatban az adatátvitel titkosító kódolására használjuk. A kapcsolatmenedzser összegyűjti egy üzenetbe az A és B értékelő üzeneteket, a dátum/idő adatot és az R(A) véletlen számot (344 lépés), A közös kulcsfunkció kódolja az üzenetet a B ügynök közös kulcsával (amit A az A ügynök bizonylatával együtt megkapott) (346 lépés), és megküldi a kódolt üzenetet B ügynök B kapcsolatmenedzserének (348 lépés), B kapcsolatmenedzser veszi az üzenetet (350 lépés).

B közös kulcsfunkció dekódolja a vett üzenetet, a dekódoláshoz saját (közös kulcsnak megfelelő) egyéni kulcsát használva (352 lépés). B kapcsolatmenedzser ellenőrzi a B értékelő üzenet helyességét, azaz azt, hogy az A-tól kapott üzenet szerinti B értékelő üzenet egyezik-e az eredeti B értékelő üzenettel, amit B küldött A-nak (354 lépés). 356 lépés: B értékelő üzenet helyes? Ha ez a feltétel teljesül, akkor B kapcsolatmenedzser ezt megjegyzi, és indítja a tranzakciós kapcsolatot (358 lépés).

B kapcsolatmenedzser ezután formál és tárol egy ügynökök közötti TA/TA=R(A)xorR(B) kapcsolatkulcsot (360 lépés). Ezen a ponton A és B kapcsolatmenedzser is formált egy-egy kapcsolatkulcsot az egymás között fennálló kapcsolatban történő használatra. Ezután B dátum/idő funkció a pillanatnyi dátum/idő adatát megküldi B biztonsági menedzsernek (362 lépés). B biztonsági menedzser összeállít egy üzenetet, amely tartalmaz egy A-nak szóló, tudomásul vevő üzenetet, az A értékelő üzenetet és B dátum/idő adatát (364 lépés). Az üzenet B-től A-hoz küldése az üzenetküldő szubrutin lefuttatásával történik: kódolással védett üzenetküldés B→A (366 lépés).

A 10. ábrán az üzenetküldés protokoll folyamatábrája van feltüntetve. B ügynök szimmetrikus kulcsfunkciója kódolja az üzenetet a TA/TA kapcsolatkulcs alkalmazásával (376 lépés). B üzenetinterfész formálja az üzenetet és a gazdaprocesszor üzenetmenedzseréhez továbbítja (378 lépés). B gazda üzenetmenedzser az üzenetet A gazda üzenetmenedzserrel fennálló kapcsolatában A ügynök gazdaprocesszorába továbbítja (380 lépés). A gazda üzenetmenedzser az üzenetet A ügynök üzenet interfészéhez továbbítja (382 lépés), amely funkció az üzenetet lecsupaszítja (384 lépés). A szimmetrikus kulcsfunkció dekódolja az üzenetet a TA/TA kapcsolatkulcs alkalmazásával, azaz a kapcsolatkulcs alkalmazásával teszi kompletté az üzenetváltást (az ügynök–ügynök kapcsolatot) (386 lépés).

A 9. (9A–9E.) ábrára visszatérve: A biztonsági menedzser veszi az üzenetet, amely tartalmaz egy A-nak szóló, tudomásul vevő üzenetet, az A értékelő üzenetet és B dátum/idő adatát (368 lépés). A biztonsági menedzser ellenőrzi A értékelő üzenetet, hogy az megfelel-e annak, amit korábban A küldött B-nek (370 lépés). 372 lépés: A értékelő üzenet helyes? Ha A értékelő üzenet nem egyezik az eredetivel, A kapcsolatmenedzser megszakítja a kapcsolatot a 332–334 lépésekben. Ha A értékelő üzenet egyezik az eredetivel, tehát helyes, akkor az A kapcsolatmenedzser ezt megjegyzi, és indítja a kapcsolatot (374 lépés).

A 8. (8A–8D.) ábrára visszatérve: a kapcsolat létrejötte után A ügynök kéri és ellenőrzi a szolgálta-

tó B ügynökének igazolóadatait, a már említett US 5557518 számú szabadalmi bejelentésünkben ismertetett módon (708 lépés).

A 708 lépésben a 11. ábra szerinti „feltételek ellenőrzése" szubrutint futtatjuk le. Mindegyik szolgáltató tranzakciós eszköze tartalmaz igazoló adatokat (feltételek), amelyek azonosítják a szolgáltató tulajdonost (például NYREX, Ticketron stb.). Ilyen szolgáltatói feltételeket például egy kereskedelmi hatóság bocsát ki és egy ezzel megbízott ügynökség ellenőriz. A 188 vevő tranzakciós eszközében tárolt feltételek viszont lehetnek gépjármű-vezetői jogosítványok, bankkártyaadatok, amelyek különböző hatóságok által lettek kiadva. A 11. ábra szerint A vásárlásfunkció B vásárlásfunkciójának küld üzenetet, amelyben kéri a szolgáltató feltételeit: egy 444 lépésben A vásárlásfunkció tanúsítványt kér B-től, egy 446 lépésben szubrutin lefuttatásával kódolással védett A→B üzenetben küldi el kérését, 448 lépésben B vásárlásfunkció veszi az üzenetet. B jegytartó előveszi a szolgáltatói feltételeket (tanúsítványt) (450 lépés) és a 452 lépésben elküldi azt A-nak ellenőrzésre. Egy 454 lépésben A biztonsági menedzser értékeli a megküldött szolgáltatói feltételeket: 456 lépés: feltételek érvényesek?

A szolgáltatói feltételek vagy bármilyen más típusú 8 jegy értékelése az alábbiak szerint történhet:

1. értékeljük a kibocsátó bizonylatát és ellenőrizzük a kibocsátó szignóját,

2. értékelünk minden transzfert, a tekintetben, hogy egyeznek-e a vevő és küldő azonosítói (azaz S_0 kibocsátó=R_0 első átvevő, aztán $R_i=S_{i+i}$, ahol $i\geq 0$,

3. értékelünk minden küldő bizonylatot és minden küldő szignót,

4. értékeljük, hogy az utolsó átvevő azonosítója egyezik-e a jelen kapcsolatban lévő ügynök bizonylatával.

Ha a szolgáltatói feltételek nem érvényesek, akkor a tranzakció megszakad a megszakító szubrutin lefuttatásával (458 lépés). A 11. ábra szerint A ügynök szakít meg a szubrutin lehívásával (458 lépés), és az A kapcsolatmenedzser küld üzenetet B ügynök kapcsolatmenedzserének arról, hogy a kapcsolat megszakad. Részletesebben: A megszakít (388 lépés), A kapcsolatmenedzser üzenetet küld: kapcsolat megszakítva (390 lépés), üzenetküldés A→B (szubrutin) (392 lépés), B kapcsolatmenedzser veszi az üzenetet (394 lépés) és B megszakítja a kapcsolatot (396 lépés). A 10. ábra szerint, ha a szolgáltatói feltételek érvényesek, akkor A gazdához funkció a feltételek információt a gazda transzfer alkalmazásnak küldi megerősítésre (például a vevő vizuálisan ellenőrzi a szolgáltató nevét és jóváhagyja) (460–462 lépések).

A 8. ábra szerint az elektronikus kereskedelmi fizetés folyamata folytatódik. A ügyfél megkérdezi: kéri-e B A feltételeit (jogosítványait)? (710 lépés). 712 lépés: üzenetküldés AΨB. B gazdához funkció üzenetet küld B gazda tranzakciós alkalmazásnak: fogadja a kereskedelmi fizetést (714 lépés). 716 lépés: Kérjük a feltételeket? Ha kérjük a vevőfeltételeket a fizető azonosítása érdekében, akkor lefuttatjuk a „feltételek ellenőrzése" szubrutint, majd B vásárlásfunkció üzenetet küld A-nak, hogy indíthatja a fizetést (720 lépés). 724 lépés: üzenetküldés BΨA. Ha a fizető azonosítására nincs szükség, akkor a B vásárlásfunkció a 724 lépésben „feltételek megküldése nem szükséges" üzenetet küld A-nak (722 lépés). B ügynök üzenetét A vásárlásfunkció fogadja egy 726 lépésben, és A gazdához funkció lekéri az átutalásiutasítás-információt A gazda tranzakciós alkalmazástól (728 lépés). A gazda tranzakciós alkalmazás az átutalásiutasítás-információt A ügynökhöz továbbítja (730 lépés), amely információt az A gazdához funkció fogad (732 lépés), és továbbít B ügynökhöz (734 lépés).

B vásárlásfunkció veszi az átutalásiutasítás-információt, értékeli az abban foglalt végösszeget, összehasonlítva a kifizetetlen számlákkal, azaz a beszedendő összeggel (736 lépés). 738 lépés: helyes az összeg? Ha az átutalásiutasítás-információ szerinti végösszeg nem helyes, a tranzakciót B megszakítja BΨA (740 lépés). Ha az átutalásiutasítás-információ szerinti végösszeg helyes, akkor B közös kulcsfunkció digitális szignóval látja el az átutalásiutasítás-információt, és szignóját B jegytartónak is megküldi (742 lépés). B jegytartó „kereskedelmi fizetés" jegyet készít (744 lépés), és megküldi a 8 jegyet A-nak (746 lépés). 748 lépés: üzenetküldés BΨA.

A vásárlásfunkció veszi és értékeli a „kereskedelmi fizetés" jegyet (750 lépés). 752 lépés: érvényes a jegy? Ha a 8 jegy érvénytelen, a tranzakciót A megszakítja AΨB (754 lépés). Ha a 8 jegy érvényes, akkor A vásárlásfunkció a 8 jegyet A jegytartóba továbbítja, és az átutalásiutasítás-információ szignóját értékelés céljából továbbadja (756 lépés).

A közös kulcsfunkció veszi és értékeli a szignót (758 lépés). 760 lépés: érvényes szignó? Ha a szignó érvénytelen, A megszakítja a tranzakciót (752, 754 lépések). Ha a szignó érvényes, akkor A vásárlásfunkció a 8 jegyet A jegytartóba helyezi, és az átutalásiutasítás-információ digitális szignóját küldi értékelésre (756 lépés).

A közös kulcsfunkció értékeli a digitális szignót, és ehhez a szolgáltató közös kulcsát alkalmazza, amit a szolgáltató feltételei között megkapott (758 lépés). 760 lépés: a szignó érvényes? Ha a digitális szignó nem helyes, A megszakítja a tranzakciót (752, 754 lépések). Ha a szignó érvényes, akkor a pénzmodulok közötti fizetés megtörténik AΨB (762 lépés).

A 762 lépésben A ügynök a korábban említett US 5557518 számú szabadalmi bejelentés szerinti módon bonyolítja le az A ügynöktől B ügynökhöz kifizetést.

A 13. (13A–13E.) ábra szerint A véletlenszám-generátor R(1) véletlen számot generál (520 lépés). A vásárlásfunkció pénzmodul fizetés és R(1) üzenetet küld B ügynöknek (522 lépés). 524 lépés: kódolással védett üzenetküldés AΨB (szubrutin). B vásárlásfunkció veszi az üzenetet (526 lépés), B biztonsági menedzser veszi R(1) véletlen számot (528 lépés), B véletlenszám-generátor R(2) véletlen számot generál és küld A biztonsági menedzsernek (530 lépés). 532 lépés: kódolással védett üzenetküldés BΨA (szubrutin). A és B biztonsági menedzserek mindegyike formál egy TA/MM=R(1)xorR(2) kapcsolatkulcsot (354, 356 lépés).

A 14. ábrán egy tranzakció során felépített, négy kódolással védett 436, 438, 440, 442 csatorna van szemléltetve. A 436 csatorna két 120 ügynök között épül fel, és TA/TA kapcsolatkulccsal kódolt üzeneteket hordoz. A 438 és 440 csatornák egy 120 ügynök és a hozzá tartozó 6 pénzmodul között épül fel, és TA/MM kapcsolatkulccsal kódolt üzeneteket hordoz. A 442 csatorna különböző 122 tranzakciós eszközök 6, 6' pénzmoduljai között épül fel és MM/MM kapcsolatkulccsal kódolt üzeneteket hordoz.

A TA/MM kapcsolatkulcs a 120 ügynök és 6 pénzmodulja közötti üzenetek rejtjelező kódolására szolgál a 438, illetve a 440 csatornában történő átvitel céljára. A folyamat azon pontján, ameddig a leírásban eljutottunk, csak a két 120 ügynöknek van TA/MM kapcsolatkulcsa. Mindkét 6, 6' pénzmodul csak a folyamat további részében fogja lemásolni a TA/MM kapcsolatkulcsot, hogy használja azt a 120 ügynökével tartandó kapcsolatban.

Megjegyzendő, hogy a 120 ügynök és 6 pénzmodulja lehetnek különálló, mechanikusan feltörés ellen védett, külön tokokba zárt egységek helyett közös tokban elrendezett 122 tranzakciós eszközök is, amely esetben nem szükséges kódolással védett kapcsolatot létesíteni a 120 ügynök és 6 pénzmodulja között. A különálló 120 ügynök és 6 pénzmodul kialakításnak azonban előnye a nagyobb mobilitás, a pénzmodul jobb hordozhatósága (zsebben elfér).

A 13. ábra szerint A pénzmodulhoz funkció „fizess" üzenetet és R(1) véletlen számot küld A pénzmodulhoz (538 lépés). Ugyanakkor B pénzmodulhoz funkció R(2) véletlen számot és „fogadd a fizetést" üzenetet küld B pénzmodulhoz (540 lépés). A pénzmodul veszi az üzenetet (542 lépés), B pénzmodul is veszi a neki szóló üzenetet (544 lépés).

Ekkor (az ügynökön belüli) A pénzmodul és B pénzmodul kapcsolatot létesítenek egymással úgy, hogy mindkét 6, 6' pénzmodul megszerzi az MM/MM kapcsolatkulcsot (546 lépés). A pénzmodul-pénzmodul kapcsolat felépítése során a pénzmodulok üzeneteket váltanak a 120 ügynökök között már meglévő kapcsolaton át. A 15. ábra szerinti 442 csatorna kapcsolatkulcsa a kódolt 436 csatornán át történő üzenetváltás során alakul ki. Így a pénzmodulok közötti kapcsolatban küldött üzenetek, legalábbis a 120 ügynökök közötti csatornában kétféle kódolással lesznek ellátva: egyrészt a pénzmodulok közötti MM/MM kapcsolatkulccsal, másrészt a ügynökök közötti kapcsolat TA/TA kapcsolatkulcsával.

Egy előnyös kialakításban a 6, 6' pénzmodulok közötti kapcsolat ugyanúgy épül fel, mint a 120 ügynökök közötti kapcsolat. Mindegyik pénzmodulnak van saját azonosító bizonylata és van közös kulcsa, amelyek tárolva vannak benne. A bizonylatok és véletlen számok (XOR) cseréje lehetővé teszi pénzmodulok közötti, biztonságos MM/MM kapcsolatkulcs alkotását. (A kapcsolatprotokollt lásd Az US 5799087 számú szabadalmi bejelentésünkben és a 15. ábrán.) A 15. ábra szerint A biztonsági őr a modul bizonylatát a kapcsolatmenedzserhez küldi (1464 lépés), A kapcsolatmenedzser ellenőrzi, hogy A pénzmodul a hálózaton van-e (1466 lépés). 1468 lépés: pénzmodul a hálózatra van kapcsolva? Ha A pénzmodul a hálózatra van kapcsolva, akkor A kapcsolatmenedzser A pénzmodul bizonylatát B-hez küldi (1476 lépés).

Ha viszont A pénzmodul nincs a hálózatra kapcsolva, akkor A szimmetrikus kulcsfunkció kódolja A pénzmodul bizonylatát egy K kulccsal (1470 lépés), A kapcsolatmenedzser a kódolt bizonylatot hálózati szerverhez küldi (1472 lépés), a hálózati szerver dekódolja a bizonylatot K kulccsal, és B-hez küldi (1474 lépés).

Függetlenül attól, hogy a bizonylatot a hálózati szervertől vagy A kapcsolatmenedzsertől kapta, B kapcsolatmenedzser veszi a bizonylatot (1480 lépés), és továbbadja B biztonsági őrnek, B biztonsági őr (ha B egy biztonsági őr, akkor a biztonsági szerver látja el ezt a feladatot) veszi és értékeli a bizonylatot (1482 lépés). 1484 lépés: bizonylat érvényes? Ha a bizonylat nem érvényes, B kapcsolatmenedzser megjegyzi, hogy a kapcsolat megszakadt, és informálja vagy a vevőt, vagy a bankot: 1486 lépés: B kapcsolatmenedzser megjegyzi: kapcsolat megszakítva, 1488 lépés: van-e folyamatban pénzmodul tranzakció?, 1490 lépés: B szolgáltatóhoz üzenet: tranzakció megszakítva, 1492 lépés: B bankhoz üzenet: tranzakció megszakítva. Ha B egy biztonsági szerver, akkor B csupán megjegyzi a tranzakció megszakadását.

Ha A pénzmodul bizonylata érvényes, akkor B biztonsági őr megvizsgálja, A pénzmodul nincs-e a megbízhatatlanok listáján (1494 lépés). 1496 lépés: A a megbízhatatlanok listáján van? Ha A pénzmodul rajta van a megbízhatatlanok listáján, akkor a kapcsolat megszakad. Ha a pénzmodul nincs a megbízhatatlanok listáján, akkor B véletlenszám-generátor R(B) véletlen számot és B értékelő üzenetet generál (1498 lépés). B óra/időzítő idő- és dátumadatot ad B biztonsági őrnek (1500 lépés). B biztonsági őr összegyűjti egy üzenetben R(B) véletlen számot, B értékelő üzenetet és a dátum/idő adatot (1502 lépés). B közös kulcsfunkció kódolja az üzenetet A közös kulcsával (1504 lépés), B kapcsolatmenedzser ehhez a kódolt üzenethez B bizonylatát hozzáfűzi, és A-nak küldi (1506 lépés).

A kapcsolatmenedzser veszi az üzenetet (1508 lépés), A közös kulcsfunkció dekódolja az üzenet kódolt részét (1510 lépés). A biztonsági őr értékeli a bizonylatot (1512 lépés). 1514 lépés: bizonylat érvényes? Ha a bizonylat nem érvényes, A kapcsolatmenedzser megjegyzi a kapcsolat megszakadását (1516 lépés), és megnézi, van-e folyamatban pénzmodul tranzakció (1518 lépés), A ügyfélhez üzenet: a tranzakció megszakítva (1520 lépés) vagy A bankhoz üzenet: tranzakció megszakítva (1522 lépés). Ha a bizonylat érvényes, A biztonsági őr ellenőrzi, B azonosítója nincs-e a megbízhatatlanok listáján (1524 lépés). 1526 lépés: B a megbízhatatlanok listáján van? Ha B a megbízhatatlanok listáján van, a kapcsolat megszakad. Ha B nincs a megbízhatatlanok listáján, akkor A biztonsági őr lehívja a dátum/idő adatot és összehasonlítja B dátum/idő adatával (1528 lépés). 1530 lépés: dátumeltérés tűréshatáron túl? Ha a dátum egy adott tűréshatáron belül nem egyezik, a kapcsolat megszakad.

Ha a dátum egy adott tűréshatáron belül egyezik, A véletlenszám-generátor R(A) véletlen számot és A értékelő üzenetet generál (1532 lépés). A biztonsági őr R(A)xorR(B) kapcsolatkulcsot képez (1534 lépés). B közös kulcsfunkciója az A értékelő üzenetet, a B értékelő üzenetet, a dátum/idő adatot és R(A) véletlen számot egy üzenetbe gyűjti (1534 lépés), A közös kulcsfunkció kódolja az üzenetet B közös kulcsával (1536 lépés), A kapcsolatmenedzser a kódolt üzenetet B-nek küldi (1538 lépés).

B kapcsolatmenedzser veszi az üzenetet (1540 lépés), B közös kulcsfunkció dekódolja az üzenetet (1542 lépés), B biztonsági őr ellenőrzi B értékelő üzenetet (1544 lépés). 1546 B értékelő üzenet korrekt? Ha B értékelő üzenet korrekt, akkor B biztonsági őr R(A)xorR(B) kapcsolatkulcsot képez, lehívja az óra/időzítő dátum/idő adatát és összehasonlítja azt A dátum/idő adatával (1548 lépés). 1550 lépés: dátumeltérés kívül van a tűréshatáron? Ha a dátum egy adott tűréshatáron belül nem egyezik, a kapcsolat megszakad. Ha a dátum egy adott tűréshatáron belül egyezik, B kapcsolatmenedzser megjegyzi a kapcsolat megnyitását (startját) (1552 lépés).

B kapcsolatmenedzser tudomásul vevő és A értékelő üzenetet küld (1554 lépés). 1556 lépés: kódolással védett üzenetküldés BΨA. A kapcsolatmenedzser veszi a tudomásul vevő és A értékelő üzenetet (1558 lépés), A biztonsági őr ellenőrzi az A értékelő üzenetet (1560 lépés). 1562 lépés: A értékelő üzenet korrekt? Ha az A értékelő üzenet nincs rendben, a kapcsolat megszakad. Ha az A értékelő üzenet korrekt, akkor A kapcsolatmenedzser megjegyzi a kapcsolat kezdetét (1564 lépés).

A pénzmodulos rendszer biztonságának átfogó felügyelete integrálható a 120 ügynökök biztonságának felügyeleti rendszerébe, de előnyösen attól függetlenül van kialakítva, amivel növelhető a rendszer biztonsága és főként a flexibilitása.

A 13. ábra szerint A pénzmodul (R1) véletlen számot küld B pénzmodulhoz (548 lépés). Ezt a lépést kezdeményezheti a pénzmodul (MM) A biztonsági őre (lásd US 5453601 számú leírásunkat, ennek módosításait és az US 5557518 számú leírásunkat, ahol a pénzmodul (MM) funkciókat MM jelzéssel különbözettük meg).

Az R(1) véletlen számot egy „irányított üzenetküldés" szubrutin lefuttatásával A pénzmodulból B pénzmodulba küldjük (550 lépés). A 16. ábra szerint A pénzmodul közös kulcsfunkciója kódolja az üzenetet (R1)-et is egy MM/MM kapcsolatkulccsal (640 lépés). A pénzmodul kapcsolatmenedzsere üzenetet küld A gazda üzenetmenedzsernek (642 lépés), amely A gazda üzenetmenedzser üzenetet küld A üzenet interfésznek (644 lépés). A üzenet interfész üzenetet küld B üzenet interfésznek (646 lépés) AΨB üzenetküldés szubrutin lefuttatásával (648 lépés), amely szubrutin kódolja, majd dekódolja az üzenetet a TA/TA kapcsolatkulccsal a 120 ügynökök közötti átvitelhez. B üzenet interfész azután üzenetet küld B gazda üzenetmenedzsernek (650 lépés), B gazda üzenetmenedzser üzenetet küld B pénzmodulnak (652 lépés). B pénzmodul kapcsolatmenedzsere veszi az üzenetet (654 lépés), B pénzmodul szimmetrikus kulcsfunkciója dekódolja az üzenetet MM/MM kapcsolatkulcs alkalmazásával (656 lépés).

A 13. ábra szerint B pénzmodul biztonsági őre TA/MM=R(1)xorR(2) kapcsolatkulcsot formál és az R(2) véletlen számot A pénzmodulnak küldi (552 lépés). 554 lépés: irányított üzenetküldés BΨA. A pénztármodul biztonsági őr is TA/MM=R(1)xorR(2) kapcsolatkulcsot formál (556 lépés). A folyamatnak ezen a pontján három kapcsolat áll fenn (14. ábra): MM/MM, MM/TA és TA/TA kapcsolatok, azaz mind a négy kódolt csatorna használatban van.

A 13. ábra szerint az A pénzmodul A előfizetőhöz funkciója felhívja (promt) A ügynököt összeg (a kiválasztott áru ára) és pénznem (dollár, jen, font stb.) megadására (558 lépés). Egy, az US 5453601 számú leírásunk szerinti pénzmodul közvetlenül az előfizetőhöz (a pénzmodul birtokosához) fordult volna, a jelen találmány szerint a pénzmodul A ügynökön át kommunikál az előfizetővel. Itt a 120 ügynök szállítja az összeg- és pénznemadatokat, amelyeket előbb beszerzett a 2 vevő ügynöke (illetve a tranzakciós eszköz) előfizetőjétől.

A 6' pénzmodul 120 ügynökhöz a promt üzenetküldés egy „küldj MM/TA üzenetet" szubrutin lefuttatásával történik (560 lépés).

A 17. ábra szerint az A pénzmodul szimmetrikus kulcsfunkciója a TA/MM kapcsolatkulcs alkalmazásával kódolja az üzenetet (658 lépés), A pénzmodul kapcsolatmenedzsere elküldi az üzenetet A ügynök üzenet interfészének A gazda üzenetmenedzser útján: 660 lépés: A pénzmodul kapcsolatmenedzsere üzenetet küld gazdához, gazda üzenetmenedzser üzenetet küld A üzenetmenedzsernek (662 lépés), A üzenet interfész veszi az üzenetet (664 lépés). A szimmetrikus kulcsfunkció dekódolja az üzenetet a TA/MM kapcsolatkulccsal (666 lépés).

A 13. ábra szerint A vásárlásfunkció megadja az összeget és pénznemet a pénzmoduljának (562 lépés) a TA/MM üzenetküldés szubrutin lefuttatásával (564 lépés). A pénzmodul fizet/vált funkciója veszi az összeg- és pénznem-információt (566 lépés).

A 18. ábra (TA/MM üzenetküldés szubrutin) szerint A szimmetrikus kulcsfunkció kódolja az üzenetet TA/MM kapcsolatkulccsal (668 lépés), A üzenet interfész az üzenetet gazda üzenetmenedzseren át (670 lépés) A pénzmodul kapcsolatmenedzserének küldi (672 lépés). A pénzmodul kapcsolatmenedzser veszi az üzenetet (674 lépés), A pénzmodul szimmetrikus kulcsfunkciója TA/MM kapcsolatkulcs alkalmazásával dekódolja az üzenetet (676 lépés).

A 13. ábra szerint A pénzmodul bankjegykönyvtára ellenőrzi, van-e a 6 pénzmodulban a kifizetéshez szükséges összegű betét (568 lépés). 570 lépés: van elég pénz? Ha nincs elegendő pénz, a tranzakció megszakad A és B pénzmodulok között: előbb A pénzmodul A előfizetőtől új összeg megadását kéri (MM/TA üzenet) egy 572 lépésben. 574 lépés: MM/TA üzenetküldés (szubrutin), A vásárlásfunkció üzenetben kéri az új összeg megadását (576 lépés). 578 lépés: TA/MM üzenet elküldése (szubrutin). 580 lépés: van megadva új összeg? A pénzmodul szubrutin lefuttatásával megszünteti a kapcsolatot B pénzmodullal (582 lépés).

Az 582 lépésben alkalmazható kapcsolatmegszüntető protokoll van ismertetve például az US 5799087 számú szabadalmi leírásunkban és jelen bejelentés szerinti 19. (19A–19B.) ábrán. A 19. ábra szerinti szubrutinban X kapcsolatmenedzser visszafejti a meghiúsult tranzakció során végzett változtatásokat, és megjegyzi, hogy a kapcsolat megszűnt (1726 lépés). X kapcsolatmenedzser ezután ellenőrzi, ment-e „lezárásra kész" üzenet (1728 lépés). 1730 lépés: „lezárásra kész" üzenet elküldve? Ha igen, X felfrissíti transzfer log-ját (1732 lépés) feljegyezve, hogy X megszakított, miután elküldte a „lezárásra kész" üzenetet, és feljegyezte a bankjegy transzferprotokoll futása során kapott mindegyik bankjegy azonosítóját és összegét a transzferlistába. Amikor tehát egy megszakítás (hibás lezárás) szubrutin előhív egy megszakítás szubrutint, a megszakításprotokoll mindig hozzáfűz információt a tranzakció log-hoz.

Ha X egy tranzakciós modul, és a „lezárásra kész" üzenet elküldésre került, akkor X előfizetőhöz funkció informálja előfizetőjét, hogy a tranzakció valószínű pénztranszferhiba miatt meghiúsult: 1734 lépés: van-e folyamatban pénzmodul tranzakció? 1736 lépés: üzenet elküldve? X előfizetőhöz: tranzakció meghiúsult, lehetséges pénztranszferhiba (1738 lépés). Ha X egy banki pénztármodul, akkor X bankhoz funkció informálja a bankot, hogy vissza kell fejtenie a tranzakciók könyvelését is: 1740 lépés: van-e folyamatban banki pénztármodul tranzakció? 1742 lépés: X bankhoz: tranzakció könyvelését visszafejteni. Ha X egy tranzakciós pénzmodul, és nem volt „lezárásra kész" üzenet küldve, akkor X előfizetőhöz funkció informálja az előfizetőt, hogy a tranzakció megszakadt (1744 lépés).

X kapcsolatmenedzser minden fenti esetben küld üzenetet Y-nak arról, hogy a tranzakció nem fejezhető be (1746 lépés). 1748 lépés: Üzenetküldés XΨY. X kapcsolatmenedzser visszafejti a változásokat, és megjegyzi a kapcsolat megszakadását (1750 lépés). Y megnézi, van-e folyamatban pénzmodul tranzakció (1752 lépés), és informálja előfizetőjét arról, hogy a tranzakció meghiúsult (1754 lépés), vagy 1756 lépés: van-e folyamatban banki pénztármodul tranzakció? 1758 lépés: Y bankhoz informálja a bankot, meghiúsult tranzakciót visszakönyvelni!

Amint azt említettük, ha egy tranzakciós kapcsolat a sikeres lezárás előtt megszakad, bankjegyek vagy más jegyek duplikációja vagy elvesztése következhet be. Elvesztés akkor következhet be, ha például az elektronikus bankjegy átutalást átvevő akkor szakít meg, amikor az átutaló lezárta a kapcsolatot. Ilyen esetben a pénzt átvevő modul feljegyzi a kétes bankjegyek adatait, és értesíti előfizetőjét, hogy a pénz átvételével esetleg probléma van (nem kapta meg A „kereskedelmi fizetési" jegyét). Megjegyzendő, hogy az átutaló pénzmodul ez esetben rendesen átutalta a pénzt.

Az átutalást átvevő pénzmodul előfizetője ezt az elveszett pénzt a bizonylatoló (engedélyező) hatóságtól követelheti. A követelésnek tartalmaznia kell a meghiúsult tranzakció transzfer log feljegyzéseit. A bizonylatoló hatóság egyeztet a bankjegyeket kibocsátó bankkal arról, hogy nem kerültek-e ki a forgalomból az érintett bankjegyek. Egy meghatározott várakozási idő leteltével, ha a bankjegyeket nem vonták be, az előfizető kérelmére visszakapja az elveszett összeget.

A 13. ábra szerint az A és B pénzmodulok közötti üzenetváltások E-irányított üzenet szubrutin lefuttatásával kerültek átvitelre, amely szubrutin használja mindhárom (MM/MM, TA/MM, TA/TA) kapcsolatkulcsot. A 20. ábra szerint A pénzmodul szimmetrikus kulcsfunkciója kódolja az üzenetet MM/MM kapcsolatkulccsal (678 lépés), majd a kódolt üzenet elküldés előtt az MM/TA kapcsolatkulccsal történő felülkódolásnak lesz alávetve (680 lépés). A üzenet interfész az üzenetet B üzenet interfészhez küldi (682 lépés). 684 lépés: üzenetküldés AΨB. A 120 ügynökök közötti kapcsolatban az üzenet TA/TA kapcsolatkulccsal van kétszeresen kódolva. B üzenet interfész ehhez hasonló módon küld üzenetet B pénzmodul szimmetrikus kulcsfunkciójának végleges dekódolás céljából: 686 lépés: B üzenet interfész veszi az üzenetet, 688 lépés: TA/MM kódolt üzenetküldés B-nek, 690 lépés: A pénzmodul szimmetrikus kulcsfunkció dekódolja az üzenetet MM/MM kapcsolatkulccsal. A 15. ábrán fel vannak tüntetve a különböző kódolási rétegek.

A 13. ábra szerint az A és B pénzmodulok a megszakító szubrutinjaikban (582 lépés) A és B pénzmodulok üzeneteket generálnak a saját A és B ügynöküknek, informálva azokat arról, hogy megszüntették a kapcsolatot, a fizetés sikertelen volt: 584 lépés: A pénztármodul MM/TA üzenetet küld, 586 lépés: B pénzmodul MM/TA üzenetet küld. A és B kapcsolatmenedzserek meggyőződnek a fizetés sikertelenségéről és megszakítanak: 588 lépés: A kapcsolatmenedzser ellenőrzi a fizetés sikerességét, 590 lépés: B kapcsolatmenedzser ellenőrzi a fizetés sikerességét, 592 sikeres a fizetés? 594 lépés: sikeres a fizetés? 596 lépés: A megszakít, 598 lépés: B megszakít.

Ha másrészt a 2 vevő ügynökéhez tartozó pénzmodulban van elég pénz a kifizetéshez, akkor A pénzmodul fizet/vált funkciója üzenetet küld a szolgáltató pénzmoduljához, közölve az átutalás összegét és a bankjegyek típusát (600 lépés). Ezt az üzenetet E-irányított üzenetként küldi (602 lépés).

B pénzmodul veszi az üzenetet az A pénzmodultól kapott adatokkal. B pénzmodul előfizetőhöz funkciója ekkor promt üzenetet küld B ügynökhöz, a fizetendő összeg értékelését kérve (604 lépés). 606 lépés: MM/TA üzenetküldés B előfizetőhöz. B ügynök vásárlásfunkciója értékeli az összeg helyességét (608 lépés). 610 lépés: helyes az összeg? Ha a közölt összeg helyes, akkor B ügynök vásárlásfunkciója „helyes az összeg" üzenetet küld B pénzmodulnak (612 lépés), vagy „helytelen összeg" üzenetet küld (614 lépés). 616 lépés: TA/MM üzenetküldés. Az esetben, ha az összeg nem helyes, B pénzmodul informálja erről A pénzmodult E-irányított üzenetben (622 lépés). A pénzmodul erre A ügynöktől újabb összeg megküldését kéri vagy megszakítást kér: 618 lépés: helyes az újabb összeg? B ügynök vásárlásfunkciója „helytelen összeg" üzenetet küld (620 lépés). A megszakítás szubrutin az 572–582 lépésekben megszakítás történik. Pénzmodulok közötti vásárlás esetén az ügynök nem

küld újabb összegadatot, így mindkét pénzmodul és mindkét ügynök megszakít.

Ha viszont a B pénzmodul a B ügynöktől „helyes összeg" üzenetet kap (624 lépés), akkor B pénzmodul elfogadó üzenetet küld (E-irányított üzenetben) a vevő A pénztármoduljához (626 lépés), amit A pénzmodul fizet/vált funkciója vesz és az összegnek megfelelő bankjegyeket az A pénzmodul pénztartójába küldi (628 lépés), amely pénztartó alkalmazás tartalmazza és kezeli a pénz elektronikus megjelenítőjét.

Megjegyzendő, hogy az imént leírt, a fizető által kezdeményezett protokoll helyett alkalmazható a fizetést átvevő által kezdeményezett protokoll is, mint amilyen a POS-fizetés protokollja. Egy ilyen protokoll szerint a szolgáltató ügynöke utasítja pénzmoduljját a várt pénzösszeg átvételére, ezt az információt megküldik a vevő pénzmoduljának is, amely a vevő ügynökétől az üzenet értékelését kéri, és ha az összeg helyes, erről a vevő ügynöke értesíti a vevő pénzmoduljját.

A 13. ábra szerint A vevő A pénzmodulja az elektronikus bankjegyeket a szolgáltató pénzmoduljának E-irányított üzenetben, meghatározott összegben átutalja a szolgáltató B pénzmoduljába (630 lépés). A 20. ábra szerinti bankjegytranszfer protokollban (leírva az US 5799087 számú leírásunkban) X bankjegykönyvtár kiválaszt egy vagy több bankjegyet, amelyek összege a kifizetendő összeggel egyezik, frissíti a bankjegyek összegét és sorszámát, üzenetet küld a pénztartónak (bankjegytárnak) (1566 lépés). X bankjegytár veszi az üzenetet, és transzferfeljegyzést készít mindegyik bankjegyhez (1568 lépés). X közös kulcsfunkció szignót készít a bankjegyek számára (1570 lépés), X pakettmenedzser pakettet állít össze a bankjegyekből, transzferfeljegyzésekből és szignókból, a pakettet Y-hoz küldi (1572 lépés). A bankjegyek választása különböző szempontok szerint történhet: (1) a digitális szignók számának minimalizálása (a hosszú processzorfoglaltság megelőzésére), (2) a pakett méretének minimalizálása, (3) a maradó elektronikus bankjegyek lehető hosszú maradék élettartamának biztosítása (lejáratig). Az ilyen célok az alábbi bankjegytranszfer algoritmussal érhetők el: (1) meghatározandók a legkevesebb számú bankjegyet tartalmazó összeállítások, (2) meghatározandó ezen összeállítások közül melyikek igénylik a legkisebb számú transzferműveletet, (3) ha egynél több választási lehetőségünk maradt, azt választjuk, amely pénzegységre vetítve a legkevesebb érvényességi egységnapot tartalmazza. Érvényességi egységnap=a bankjegyek maradékértékének és lejáratig maradó érvényességi napjainak szorzata a pakett teljes tartalmára.

A megadott szempontok szerinti választás algoritmusa: X bankjegytár veszi az üzenetet X bankjegykönyvtártól, és feljegyzést készít mindegyik bankjegy számára (1568 lépés). X közös kulcsfunkció szignót készít a bankjegyek számára (1570 lépés). X pakettmenedzser pakettet állít össze a bankjegyekből, transzferfeljegyzésekből és szignókból, a pakettet Y pakettmenedzserének küldi (1572 lépés). Kódolással védett üzenetküldés XΨY (1574 lépés). Y pakettmenedzser veszi a pakettet és szétszedi (1576 lépés).

Y értékelő érvényesíti a bizonylatokat (azaz a pénzformátum generátor bizonylatát és minden transzfer bizonylatait), értékeli a bizonylatok transzferadatait (a korábbiakat is, megállapítva, hogy azonosító számaik egyeznek-e a küldő modulok digitális szignóba foglalt azonosítójával), a transzferösszegek konzisztenciáját bankjegyenként, és a végösszeget (1578 lépés). 1580 lépés: érvényes? Ha az értékelés nem talál mindent rendben, a tranzakció megszakad YΨX (1582 lépés).

Ha az értékelés mindent rendben és érvényesnek talál, és Y egy tranzakciós eszköz, akkor Y értékelő megvizsgálja a bankjegyek lejáratát: 1584 lépés: van-e folyamatban pénzmodul tranzakció? Ha igen, 1586 lépésben Y értékelő értékeli a lejárati dátumokat. 1588 lépés: van lejárt bankjegy? Ha bármelyik bankjegy lejárt, a tranzakció megszakad. Ha nincs lejárt bankjegy, akkor Y értékelő összevet minden transzferazonosítót a megbízhatatlanok listájával (1590 lépés), 1592 lépés: van vizsgált azonosító a listán? Ha bármelyik elektronikus bankjegy azonosítója szerepel a listán, a kapcsolat megszakad.

Ha Y értékelő nem talált rossz vagy megbízhatatlan bankjegyet (vagy Y nem egy tranzakciós eszköz), akkor Y közös kulcsfunkció értékeli a bankjegyek szignóit (1594 lépés), 1596 lépés: szignó érvényes? Ha a szignók bármelyike érvénytelen, a tranzakció megszakad. Ha a szignó(k) érvényes(ek), akkor Y értékelő összehasonlítja a bankjegytörzseket a tranzakció log szerinti bankjegytörzsekkel, és ellenőrzi, nincs-e duplikáció (1598 lépés). 1600 lépés: egyezés van? Ha az ellenőrzés kimutatott duplikált bankjegyet, a tranzakció megszakad. Ez az ellenőrzés (1598–1604 lépések) alkalmas arra, hogy a csalók kedvét elvegye az „önkiszolgálástól", attól, hogy tranzakciós eszközét úgy manipulálja, hogy azzal pénze keletkezzék duplikálás útján.

Y bankjegytár transzferfát készít a bankjegytörzsekkel, és ellenőrzi, nincs-e duplikáció (1602 lépés). 1604 lépés: van duplikáció? Ha nincs duplikált bankjegy, és a bankjegytörzsek is egyeznek, akkor Y bankjegytár a bankjegyeket tartóba helyezi (1606 lépés). Végül Y bankjegykönyvtár frissíti a bankjegyek tárolási hely- és összegadatait, sorszámot ad (1608 lépés).

Amint a fentiekből következik, az elektronikus bankjegytranszfer eljárás magába foglal frissítő és sorszámozó lépéseket is, ami lehetővé teszi a bankjegyek azonosítását, a küldő ellenőrzését a tekintetben, hogy az nincs-e a megbízhatatlanok listáján, és lehetővé teszi a duplikált bankjegyek kiszűrését. Ezek a többletjellemzők és -lépések megnehezítik a duplikált bankjegyek keletkeztetését és forgalmazását, azonnal felfedezhetővé teszik, és automatikusan kiszűrik a duplikált bankjegyet a tranzakció során.

A 13. ábra szerint Y pénzmodul lezárja a kapcsolatot egy szubrutin alkalmazásával, E-irányított üzenetben (MM YΨMM X) (632 lépés). Egy kapcsolatlezáró protokoll van szemléltetve a 22. ábrán (hasonló van ismertetve az US 5799087 számú szabadalmi bejelentésünkben). Eszerint X kapcsolatmenedzser „lezárásra kész" üzenetet ad Y-nak (1702 lépés). 1704 lépés: üzenetküldés XΨY. Ebben az üzenetben a lezárás kötele-

zettségét átruházza az üzenetet vevő modulra. Egy hagyományos pénztranszfer-folyamatban ez a kötelezettségátruházás használatos arra, hogy mindig a pénzt küldő zárja le előbb a transzferkapcsolatot, hogy ne legyen módja a pénz duplikálására.

Y kapcsolatmenedzser tudomásulvétel üzenetet küld X-nek (1706 lépés), (1708 lépés: üzenetküldés YΨX) és lezárja még nyitott kapcsolatait a transzfer log frissítésével (1710 lépés). Ha Y egy tranzakciós eszköz, akkor egy 1712 lépés: van-e folyamatban pénzmodul tranzakció? és 1714 lépésben az Y előfizetőhöz funkció tranzakció lezárult kijelzést ad az előfizető felé. Y kapcsolatmenedzser megjegyzi a kapcsolat végét (1716 lépés).

X transzfer log frissíti a transzfer log feljegyzését (1718 lépés), 1720 lépésben megnézi, van-e folyamatban pénzmodul tranzakció, ha igen, lezárja minden külső kapcsolatát, ugyanúgy, mint Y tette: X előfizetőhöz funkció tranzakció lezárult kijelzést ad előfizető felé (1722 lépés), X kapcsolatmenedzser megjegyzi, a kapcsolat lezárult (1724 lépés).

Hasonló folyamatábra szerinti protokollt alkalmazunk 6 pénzmodul és 120 ügynöke kapcsolatának lezárásánál is, azzal a különbséggel, hogy az üzenetküldés lépésben E-irányított üzenetküldés szubrutinját futtatjuk le, és hogy az előfizetőhöz funkció nem az előfizető számára ír ki üzenetet, hanem a 120 ügynök számára küld üzenetet. A fentiek szerint B pénzmodul kapcsolatmenedzsere küld „kapcsolat lezárására kész" üzenetet A pénzmodul kapcsolatmenedzserének egy E-irányított üzenetben (szubrutin: 1702–1704 lépések), A pénzmodul küld tudomásul vevő üzenetet B pénzmodulnak, és A pénzmodul lezárja a kapcsolatát (1706–1716 lépések). Amikor B pénzmodul vette a tudomásul vevő üzenetet, B pénzmodul is lezárja kapcsolatát (1718–1724 lépésekben).

A és B pénzmodulok kapcsolatát lezáró rutinok szerint A és B pénzmodul üzeneteket generálnak és küldenek a hozzájuk tartozó ügynök számára (1714, 1722 lépés), informálva őt, hogy részükről a kapcsolat le van zárva, és a fizetés sikeres volt.

A 13. ábra szerint mindkét pénzmodul az említett „sikeres fizetés" üzenetet küld a saját ügynökének (584, 586 lépések), amely üzenetek TA/MM kapcsolatkulccsal kódoltak. A kapcsolatmenedzser ellenőrzi a fizetés sikerességét (588 lépés), 592 lépés: sikeres a fizetés? B kapcsolatmenedzser is ellenőrzi a fizetés sikerességét (590 lépés), 594 lépés: sikeres a fizetés? Ha nem, akkor 596 lépésben A megszakít, 598 lépésben B megszakít. Ha az 594 lépés szerint a fizetés sikeres volt, akkor Y lezárja a kapcsolatot (638 lépés), így ha az 592 lépésben a fizetés sikeresnek bizonyult, A jegytartó frissíti az „kereskedelmi fizetési" jegyet a fizetési információval (634 lépés) és A lezárja a kapcsolatot (636 lépés), így a jegy tárolása A pénzmodulban véglegessé válik.

A 8. ábra szerinti folyamatban A jegytartó a „kereskedelmi fizetés" jegyet A gazda tranzakciós alkalmazáshoz küldi (764 lépés). A jegytartó a „kereskedelmi fizetés" jegyet veszi és továbbítja azt az átutalási utasításinformációval együtt a 189 kifizetőrendszerhez a kifizetés bizonylataként (766 lépés). B jegytartó a „kereskedelmi fizetés" jegyet B gazda tranzakciós alkalmazáshoz küldi (768 lépés). B gazda tranzakciós alkalmazás veszi a „kereskedelmi fizetés" jegyet, és a 193 fizetést elfogadó rendszerhez küldi a kifizetetlen számlákkal történő egyeztetésre (770 lépés). Ez az egyeztetés egy alternatív megoldásban már a fizetés tranzakció során lefolytatható.

SZABADALMI IGÉNYPONTOK

1. Elektronikus kereskedelmi fizetőrendszer, amelynek része a vevő (B) ügynöke (2), a vevő ügynökéhez (2) tartozó, vele védett üzenetváltásra alkalmas első pénzmodul (6), a vevő ügynökével (2) első, kódolással védett kapcsolat létesítésére alkalmas szolgáltató (A) ügynöke (4), a szolgáltató ügynökéhez (4) tartozó, vele védett üzenetváltásra alkalmas, az első pénzmodullal (6) második kódolással védett kapcsolatot létesítő, második pénzmodul (6'), *azzal jellemezve,* hogy a rendszerben

a vevő ügynöke (2) elektronikus átutalási utasításinformációt közöl a szolgáltató ügynökével (4), amely információ vételét a szolgáltató ügynöke „kereskedelmi fizetés" jegy (8) adásával visszaigazolja,

a vevő ügynöke (2) a „kereskedelmi fizetés" jegy (8) vétele után elektronikus pénzmegjelenítő első pénzmodulból (6) második pénzmodulba (6') történő kifizetését kezdeményezi.

2. Az 1. igénypont szerinti rendszer, *azzal jellemezve,* hogy a szolgáltató ügynöke (4) az átutalási utasításinformációhoz digitális szignóját fűzi, és a digitális szignót belefoglalja a „kereskedelmi fizetés" jegybe (8).

3. A 2. igénypont szerinti rendszer, *azzal jellemezve,* hogy a vevő ügynöke (2) a „kereskedelmi fizetés" jegy (8) vétele után, mielőtt kezdeményezné az elektronikus pénzmegjelenítő kifizetését, értékeli a digitális szignót.

4. A 3. igénypont szerinti rendszer, *azzal jellemezve,* hogy az átutalási utasításinformáció tartalmaz egy számlalistát (50).

5. Elektronikus kereskedelmi fizetőeljárás az 1–4. igénypontok bármelyike szerinti rendszerben történő alkalmazásra, amely rendszernek része a vevő (B) ügynöke (2), a vevő ügynökéhez (2) tartozó első pénzmodul (6), a szolgáltató (A) ügynöke (4), a szolgáltató ügynökéhez (4) tartozó második pénzmodul (6'), *azzal jellemezve,* hogy

a) kódolással védett, első kapcsolatot létesítünk a vevő ügynöke (2) és a szolgáltató ügynöke (4) között,

b) a vevő ügynökéből (2) a kódolással védett első kapcsolatban elektronikus átutalásiutasítás-információt közlünk a szolgáltató ügynökével (4),

c) amely információ vételének igazolásaként a szolgáltató ügynökével (4) „kereskedelmi fizetés" jegyet (8) készíttetünk, a „kereskedelmi fizetés" jegybe (8) belefoglalva, legalább részben, az átutalásiutasítás-információt,

d) a szolgáltató ügynökéből (4) a kódolással védett első kapcsolatban eljuttatjuk a „kereskedelmi fizetés" jegyet (8) a vevő ügynökéhez (2), amely vevő ügynöke (2) ideiglenesen tárolja a megkapott „kereskedelmi fizetés" jegyet (8),

e) az első és második pénztármodul (6, 6') között kódolással védett második kapcsolatot létesítünk,

f) amely második kapcsolatban elektronikus pénzt a szolgáltató ügynöke (4) első pénzmoduljából (6) második pénzmodulba (6') juttatunk, amely második pénzmodulban (6) az átutalt elektronikus pénzt ideiglenesen tároljuk,

g) az első pénzmodulban (6) a kapcsolat lezárását kezdeményezzük, és biztonságosan informáljuk a vevő ügynökét (2) az elektronikus pénz sikeres vételéről,

h) a második pénzmodulban (6') a kapcsolatot lezárjuk, a kapcsolat lezárásával az elektronikus pénz tárolásának ideiglenes jellegét véglegesre változtatjuk, továbbá biztonságosan informáljuk a szolgáltató ügynökét (4) az elektronikus pénz sikeres vételéről,

i) a vevő ügynökében (2) az első kapcsolatot lezárjuk, a kapcsolat lezárásával a „kereskedelmi fizetés" jegy (8) tárolásának ideiglenes jellegét véglegesre változtatjuk,

j) a szolgáltató ügynökében (4) az első kapcsolatot lezárjuk.

6. Az 5. igénypont szerinti eljárás, *azzal jellemezve,* hogy a szolgáltató ügynökében (4) az átutalásiutasítás-információhoz digitális szignót fűzünk, és a digitális szignót belefoglaljuk a „kereskedelmi fizetés" jegybe (8).

7. A 6. igénypont szerinti eljárás, *azzal jellemezve,* hogy a vevő ügynökében (2) kiértékeljük a megkapott „kereskedelmi fizetés" jegyet (8) az elektronikus pénz átutalása előtt.

8. Rendszer elektronikus kereskedelmi fizetés és átutalási utasítás összekapcsolására távközlőhálózaton, amely rendszernek része egy feltörés ellen védett, első elektronikus tranzakciós eszköz (122), amelynek első processzora van, és egy feltörés ellen védett, az első elektronikus tranzakciós eszközzel (122) biztonságos kapcsolatot tartó első pénzmodul (6), amelynek második processzora van, továbbá része egy feltörés ellen védett második elektronikus tranzakciós eszköz (122), amelynek harmadik processzora van, és egy feltörés ellen védett, a második elektronikus tranzakciós eszközzel (122) biztonságos kapcsolatot tartó és az első pénzmodullal (6) első, kódolással védett, biztonságos kapcsolat létesítésére alkalmasan kialakított, második pénzmodul (6'), amelynek negyedik processzora van, és amely második tranzakciós eszköz (122) az első tranzakciós eszközzel (122) kódolással védett kapcsolat létesítésére alkalmasan van kialakítva, *azzal jellemezve,* hogy

az első processzor elektronikus átutalásiutasítás-információ második elektronikus ügynökkel az első biztonságos kapcsolatban történő közlésére alkalmasan van kialakítva,

a harmadik processzor a megkapott átutalási információ alapján „kereskedelmi fizetés" jegy (8) készítésére és a jegy (8) első elektronikus ügynökhöz (2), első biztonságos kapcsolatban történő küldésére alkalmasan van kialakítva,

az első processzor a „kereskedelmi fizetés" jegy (8) kiértékelésére és elektronikus pénznek az első pénzmodulból (6) a második modulba (6') történő kifizetésére alkalmasan van kialakítva.

9. A 8. igénypont szerinti rendszer, *azzal jellemezve,* hogy a harmadik processzor az átutalásiutasítás-információ számára digitális szignó készítésére és a digitális szignónak „kereskedelmi fizetés" jegybe foglalására alkalmasan van kialakítva.

10. A 9. igénypont szerinti rendszer, *azzal jellemezve,* hogy az átutalásiutasítás-információ számlalistát tartalmaz.

11. A 10. igénypont szerinti rendszer, *azzal jellemezve,* hogy a számlalista szerinti számlák összegeinek végösszegét az átutalási utasításban megadott átutalandó összeggel összevető egysége van.

12. Rendszer elektronikus kereskedelmi fizetés és átutalási utasítás összekapcsolására, amely rendszernek része egy feltörés ellen védett, első elektronikus tranzakciós eszköz (122), amelynek első processzora van, és egy feltörés ellen védett, az első elektronikus tranzakciós eszközzel (122) biztonságos kapcsolatot tartó második elektronikus tranzakciós eszköz (122), amelynek második processzora van, amely második tranzakciós eszköz (122) az első tranzakciós eszközzel (122) kódolással védett kapcsolat létesítésére alkalmasan van kialakítva, *azzal jellemezve,* hogy

az első processzor elektronikus átutalásiutasítás- és számlalista-információ második elektronikus tranzakciós eszközzel (122) történő közlésére alkalmasan van kialakítva,

a második processzor az átutalásiutasítás-információ számára digitális szignó készítésére és a digitális szignónak „kereskedelmi fizetés" jegybe (8) foglalására alkalmasan van kialakítva,

a második processzor a jegy (8) első elektronikus ügynökhöz (2) első biztonságos kapcsolatban történő küldésére alkalmasan van kialakítva,

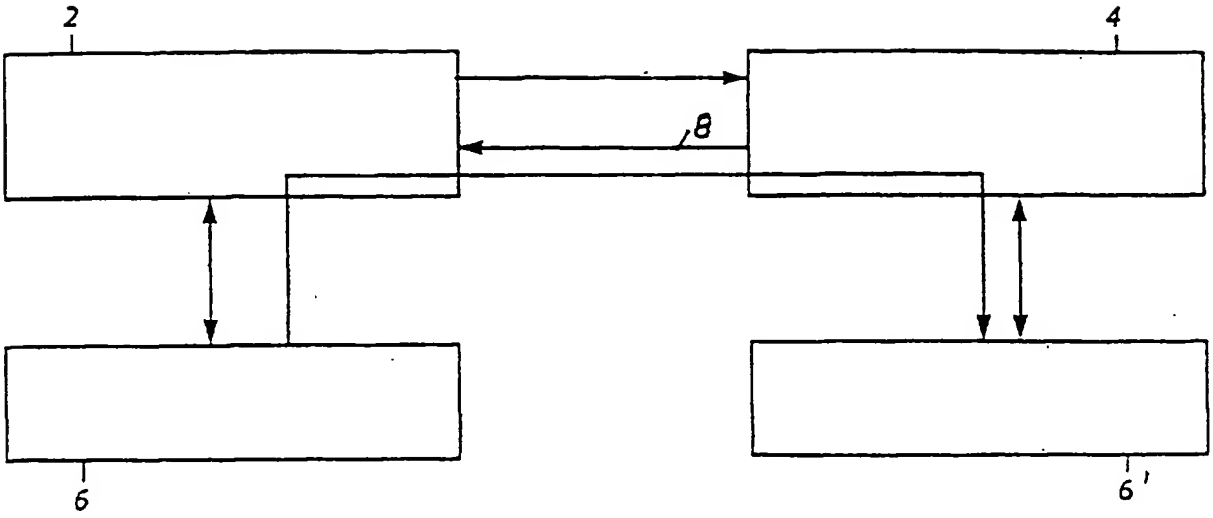
az első processzor elektronikus pénznek az első tranzakciós eszközből (122) a második tranzakciós eszközbe (122) harmadik fél közbeavatkozása nélkül történő kifizetésére alkalmasan van kialakítva.

13. A 12. igénypont szerinti rendszer, *azzal jellemezve,* hogy a „kereskedelmi fizetés" jegy (8) egy számítógépes, bankszámlás kifizetőrendszerben (189) a fizetés bizonylatát képezi.

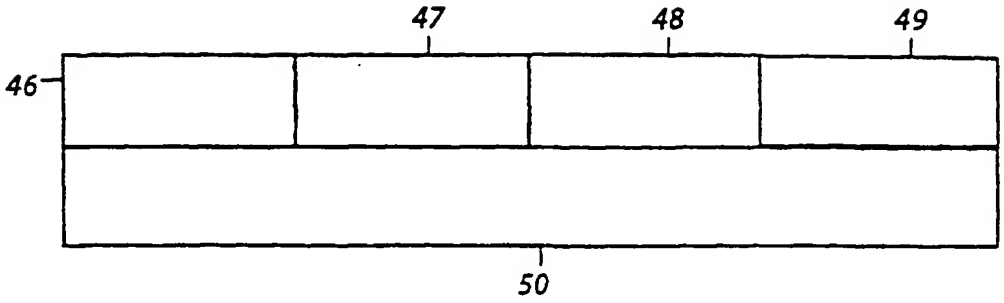
14. A 12. igénypont szerinti rendszer, *azzal jellemezve,* hogy az átutalási utasítást egy számítógépes, bankszámlás, fizetést elfogadó rendszerbe (193) kifizetetlen számlákkal történő összevetés céljából továbbító második tranzakciós eszköze (122) van.

15. A 12. igénypont szerinti rendszer, *azzal jellemezve,* hogy az első tranzakciós eszköznek (122) a digitális szignót pénz átutalása előtt értékelő egysége van.

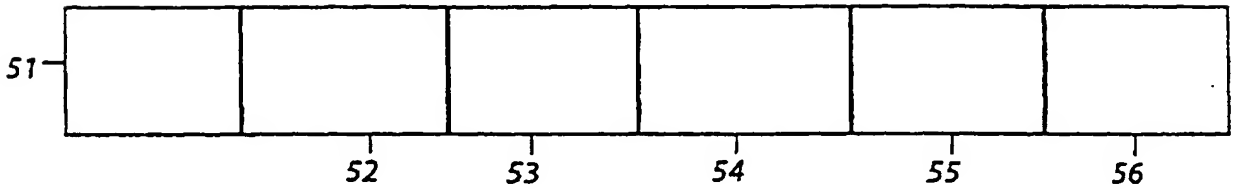
16. A 12. igénypont szerinti rendszer, *azzal jellemezve,* hogy az első tranzakciós eszköznek (122) az elektronikus szolgáltató második tranzakciós eszközéhez (122) társított feltételei érvényességét értékelő egysége van.



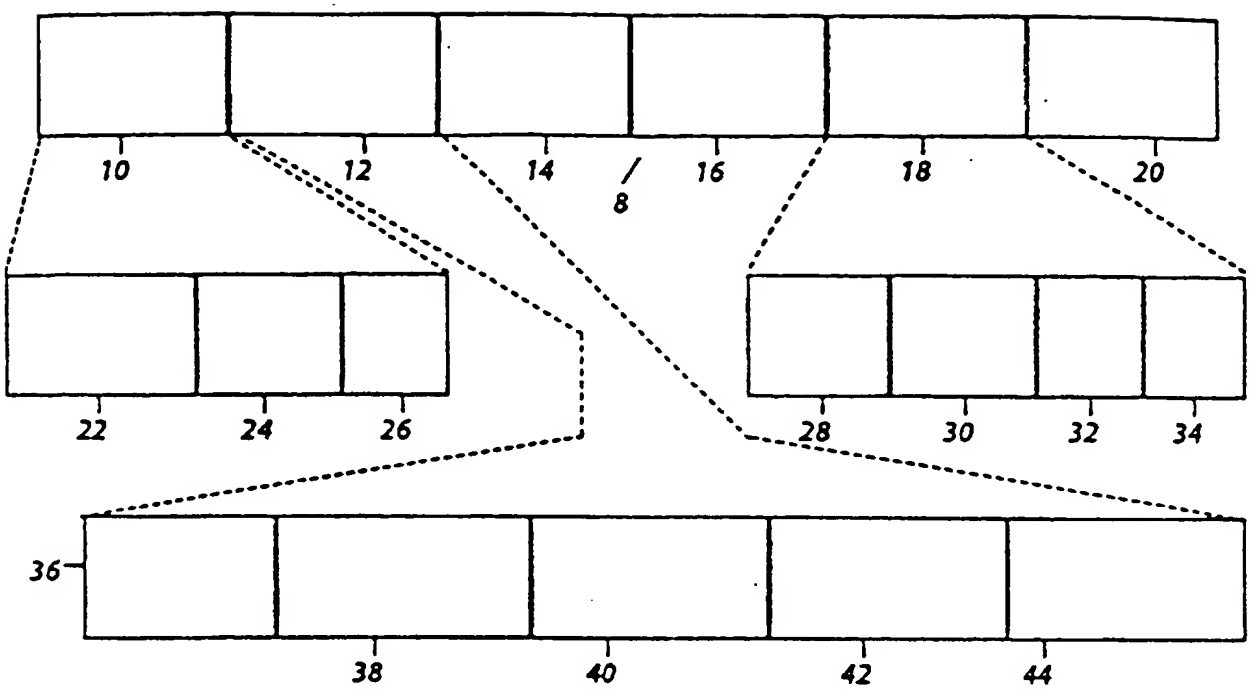
1. ábra



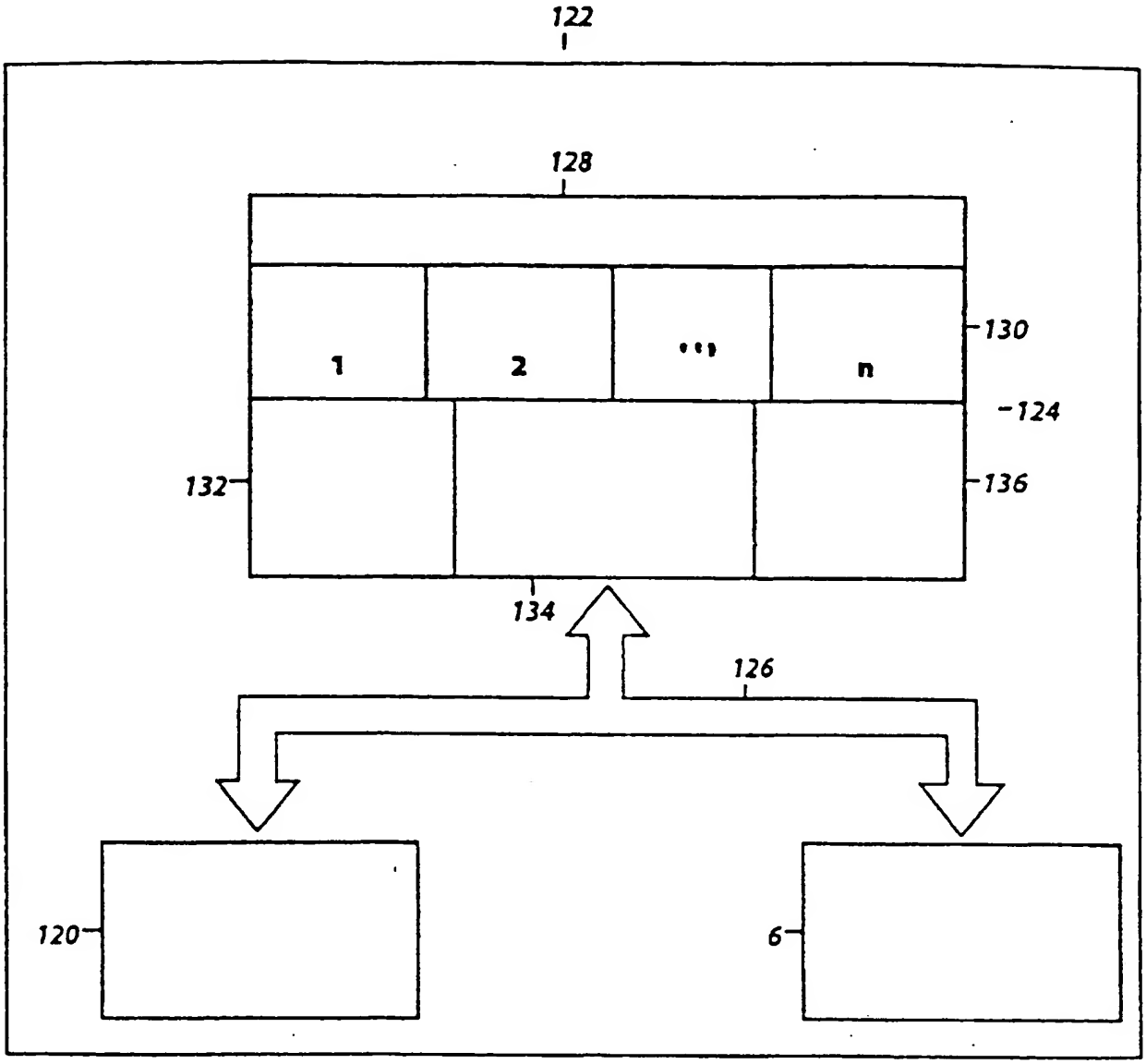
2A. ábra



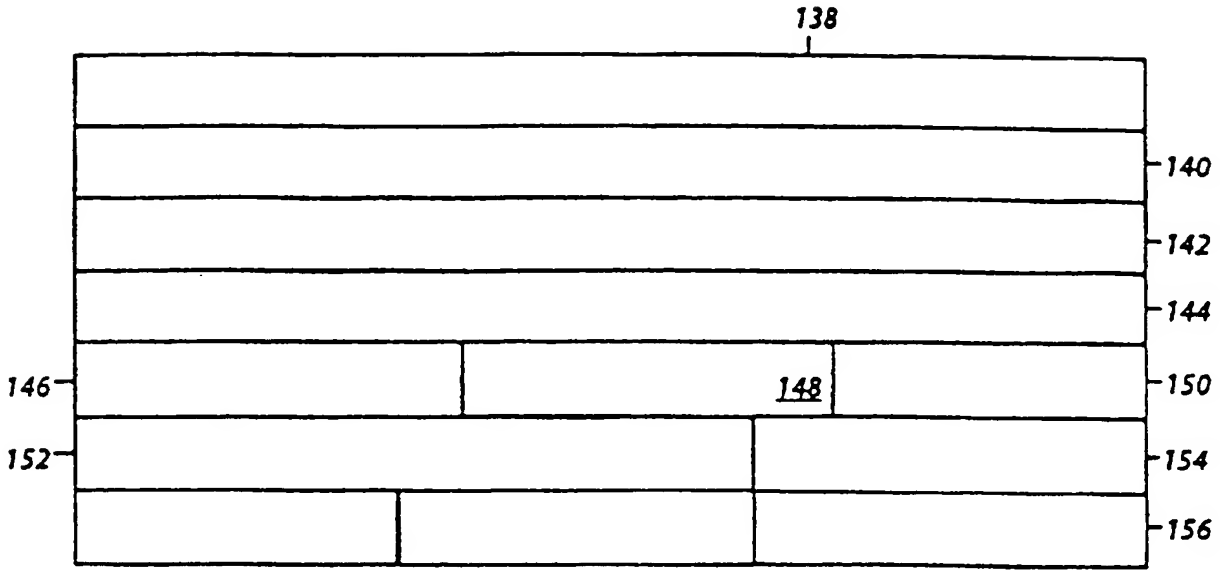
2B. ábra



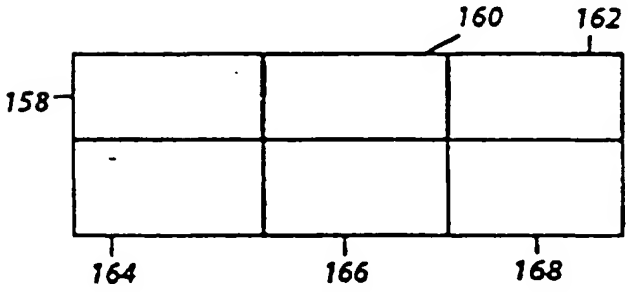
3. ábra



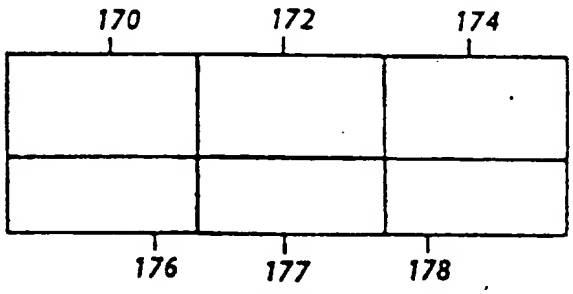
4. ábra



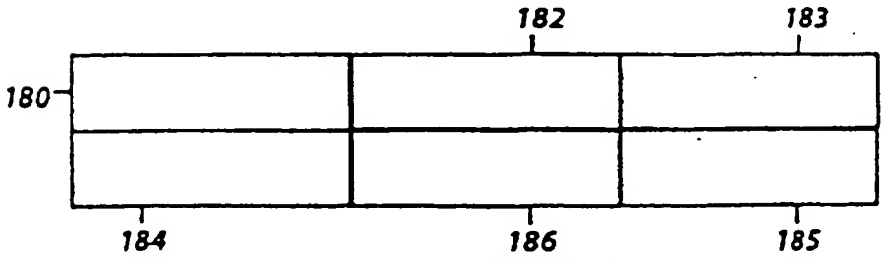
5A. ábra



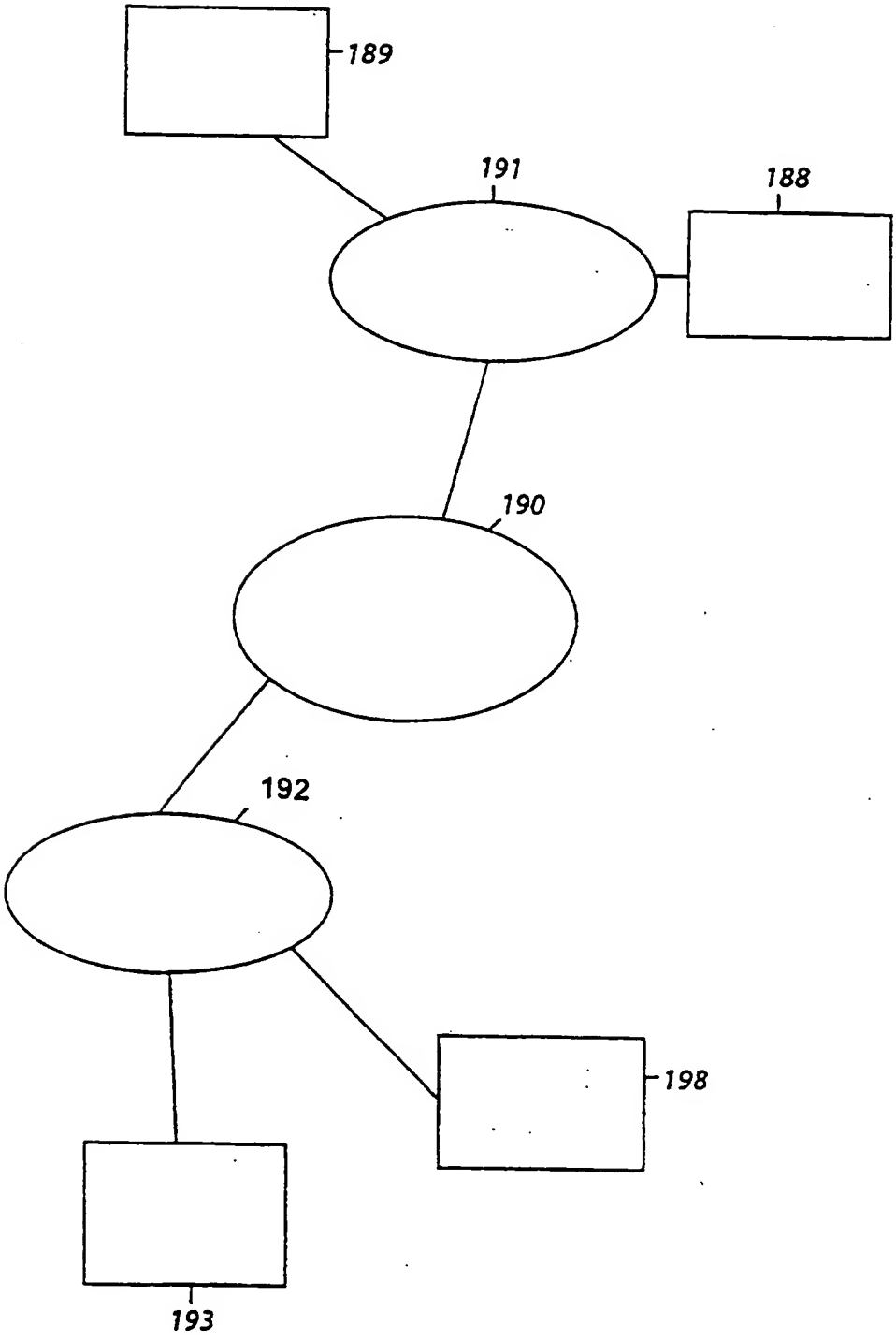
5B. ábra



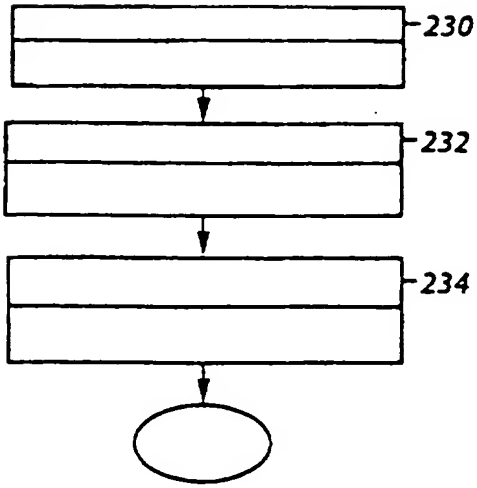
5C. ábra



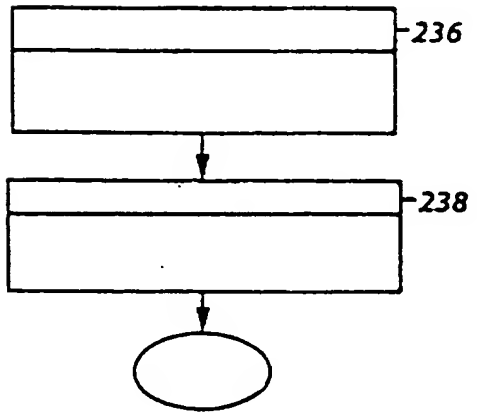
5D. ábra



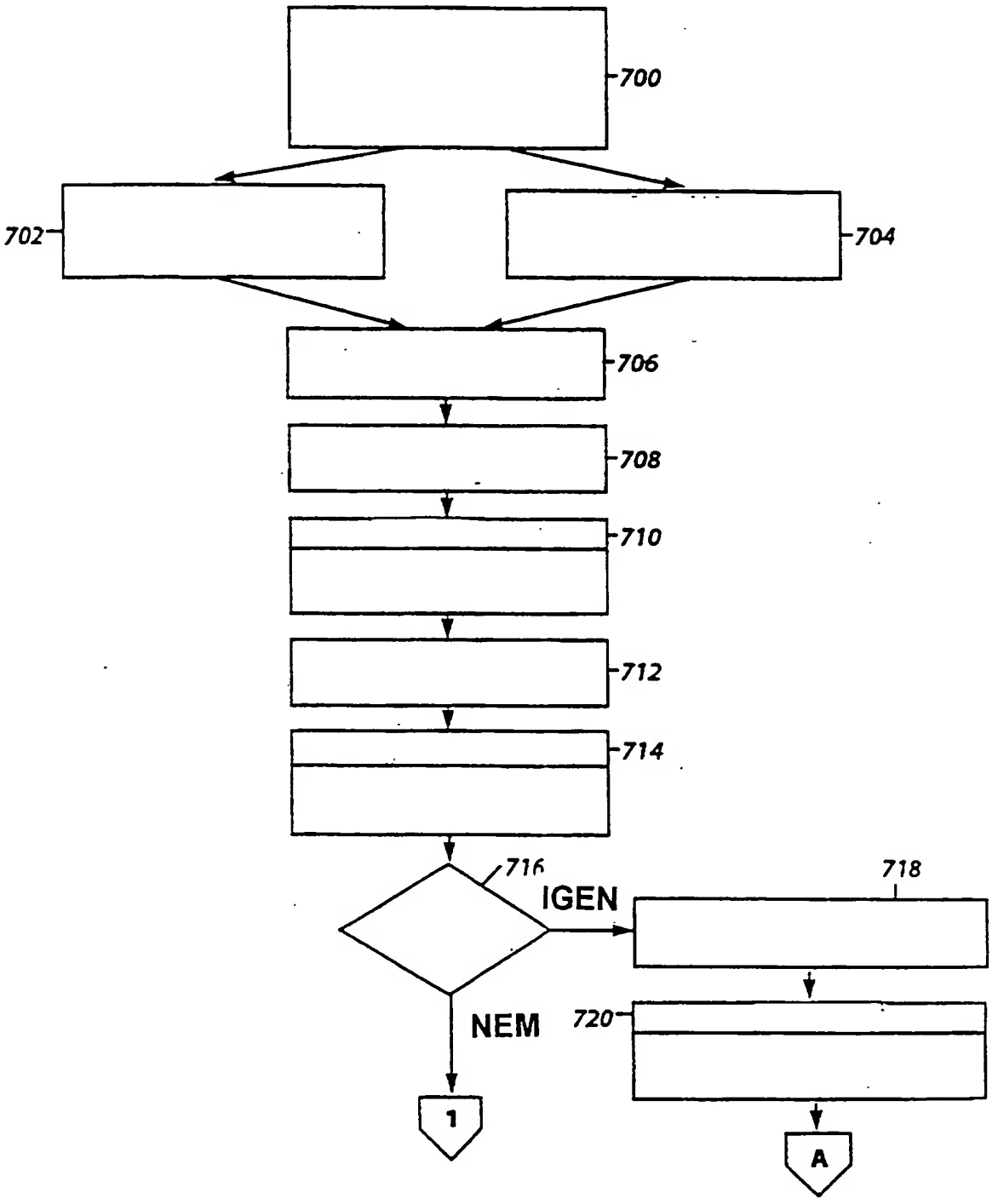
6. ábra



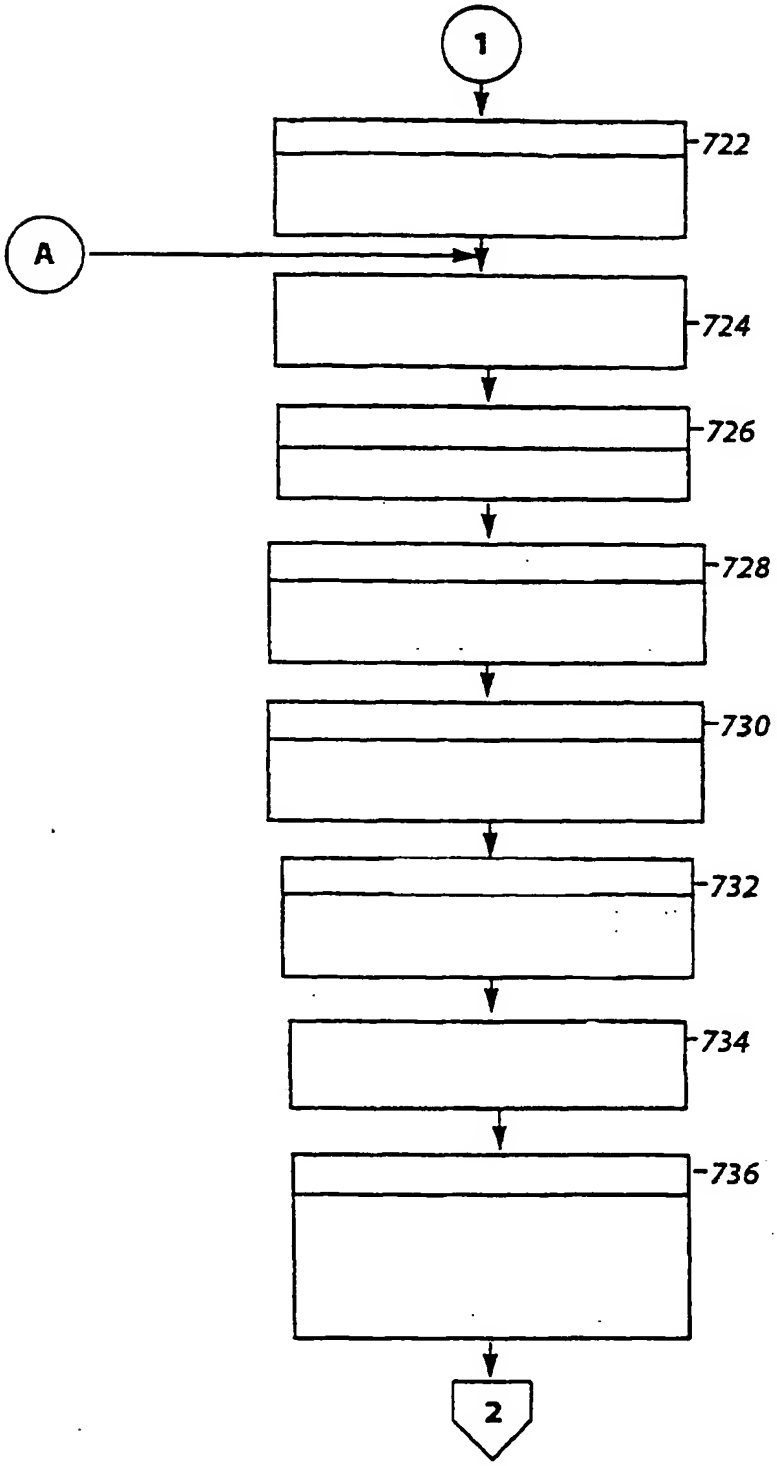
7A. ábra



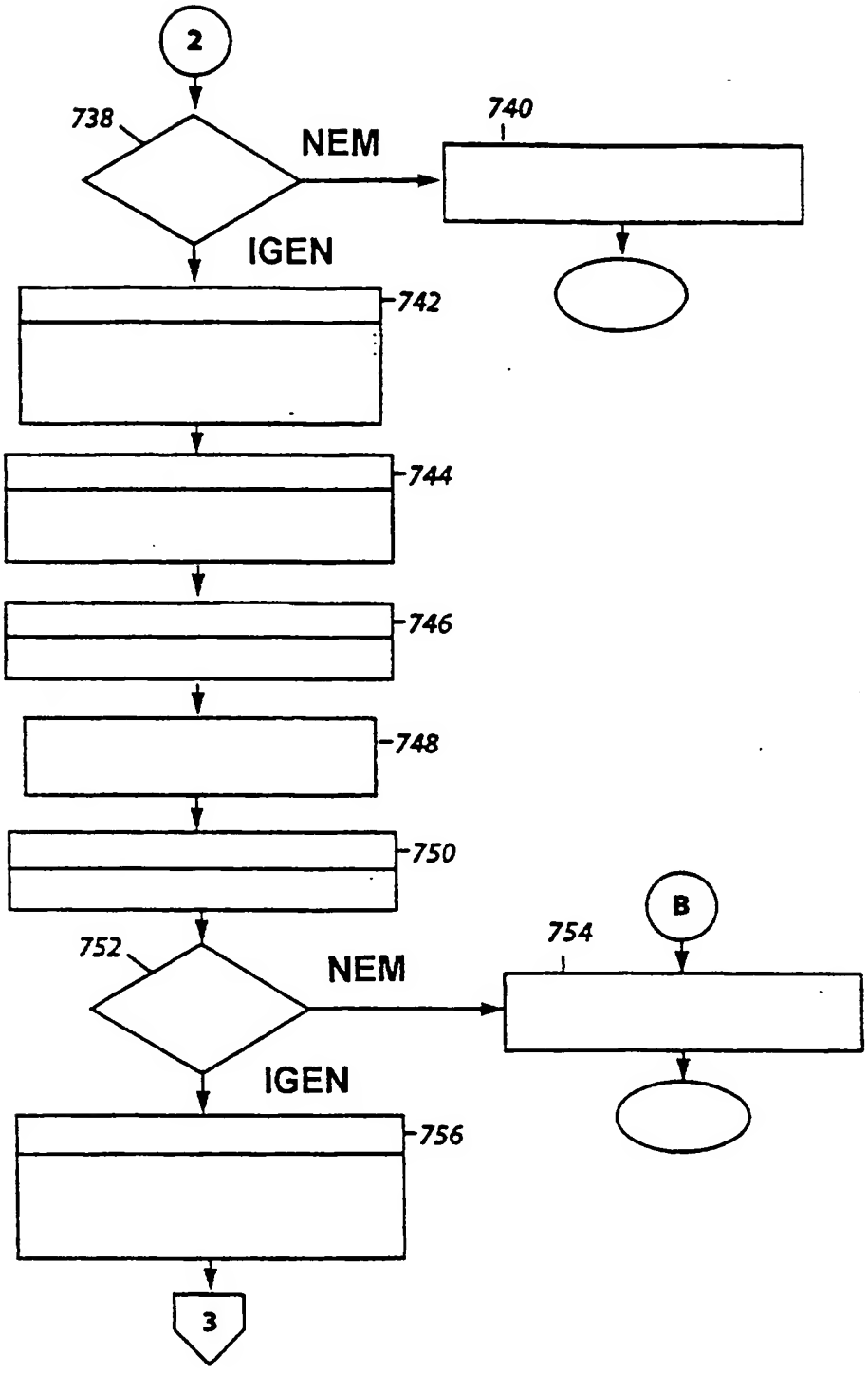
7B. ábra



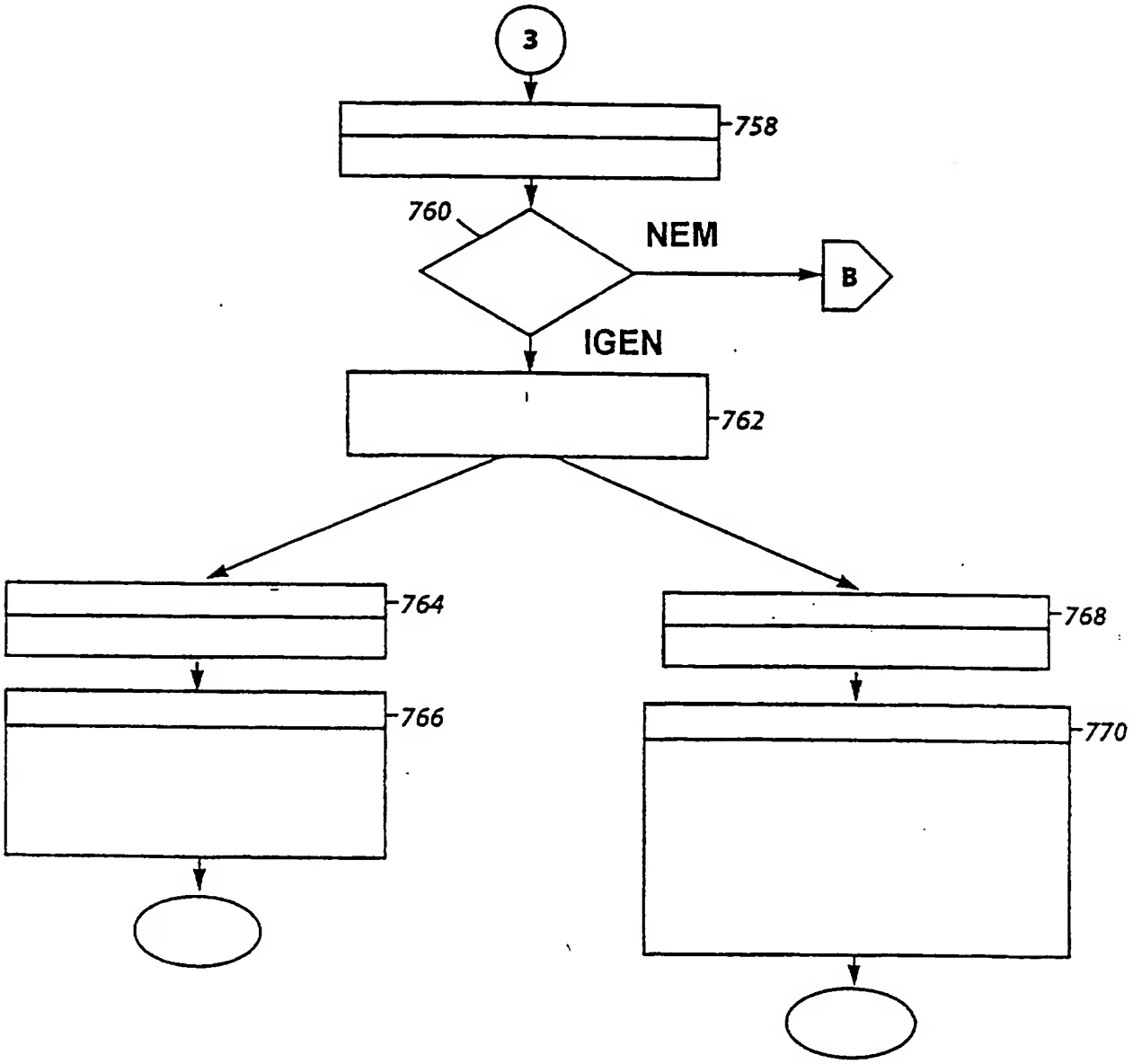
8A. ábra



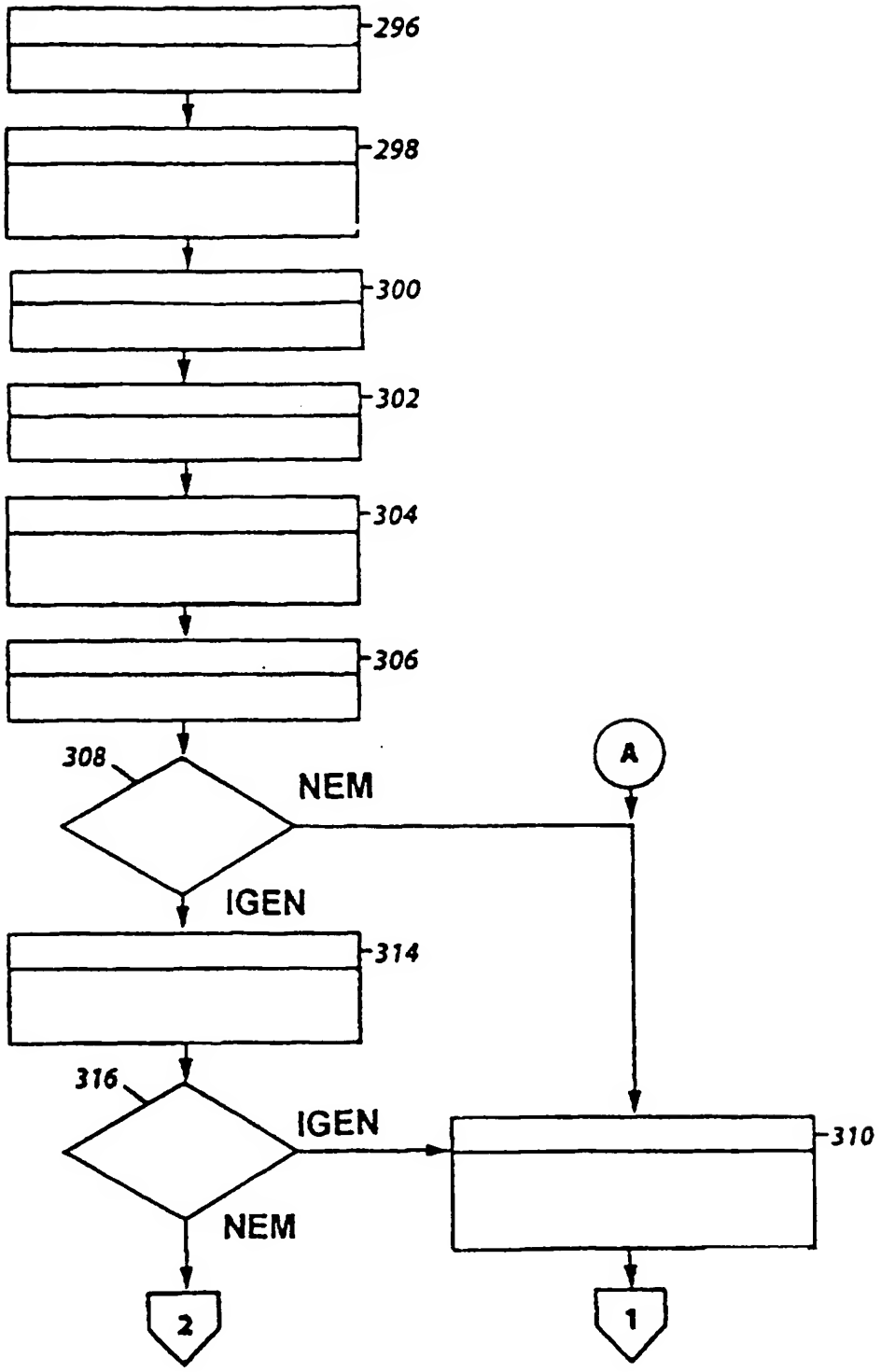
8B. ábra



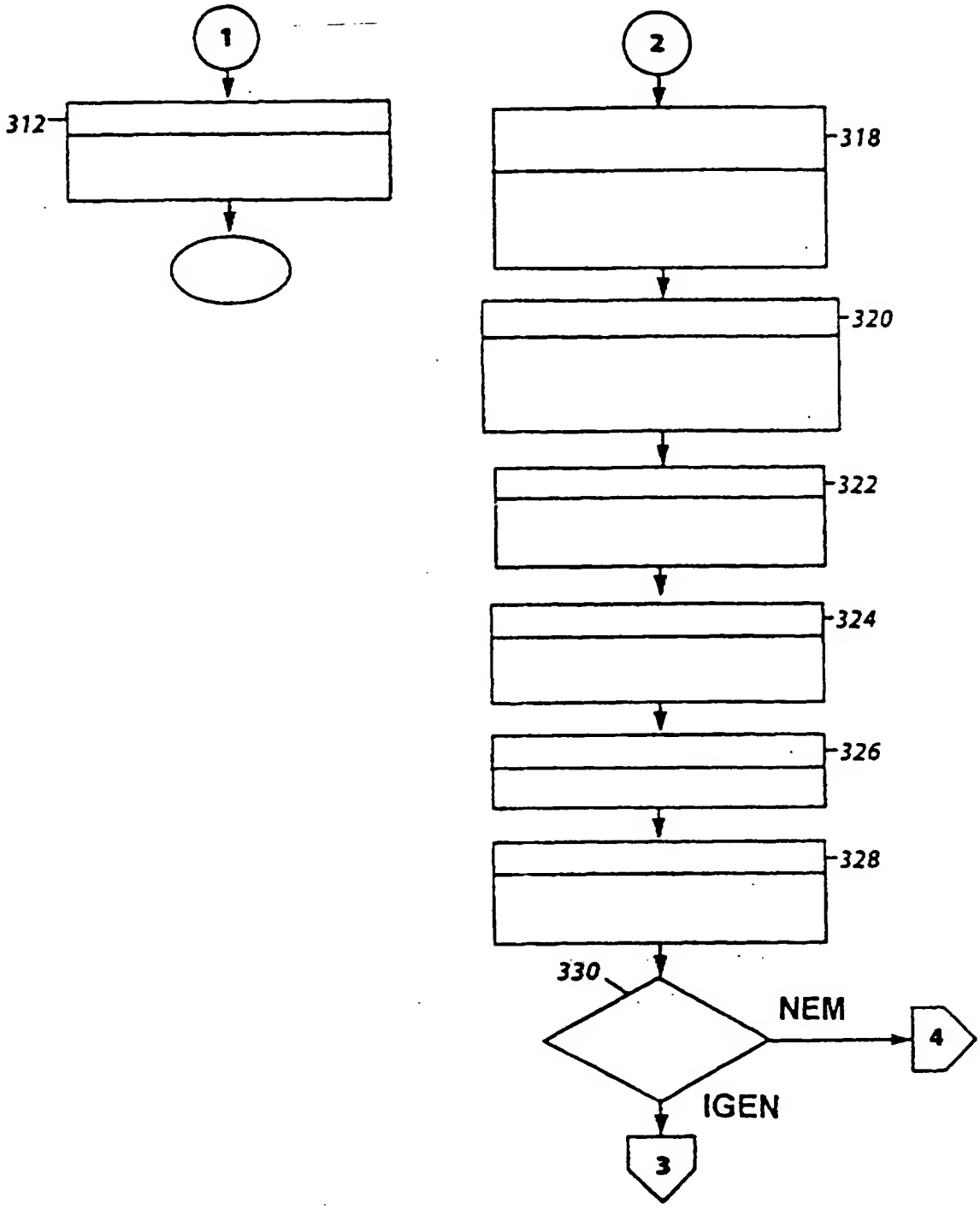
8C. ábra



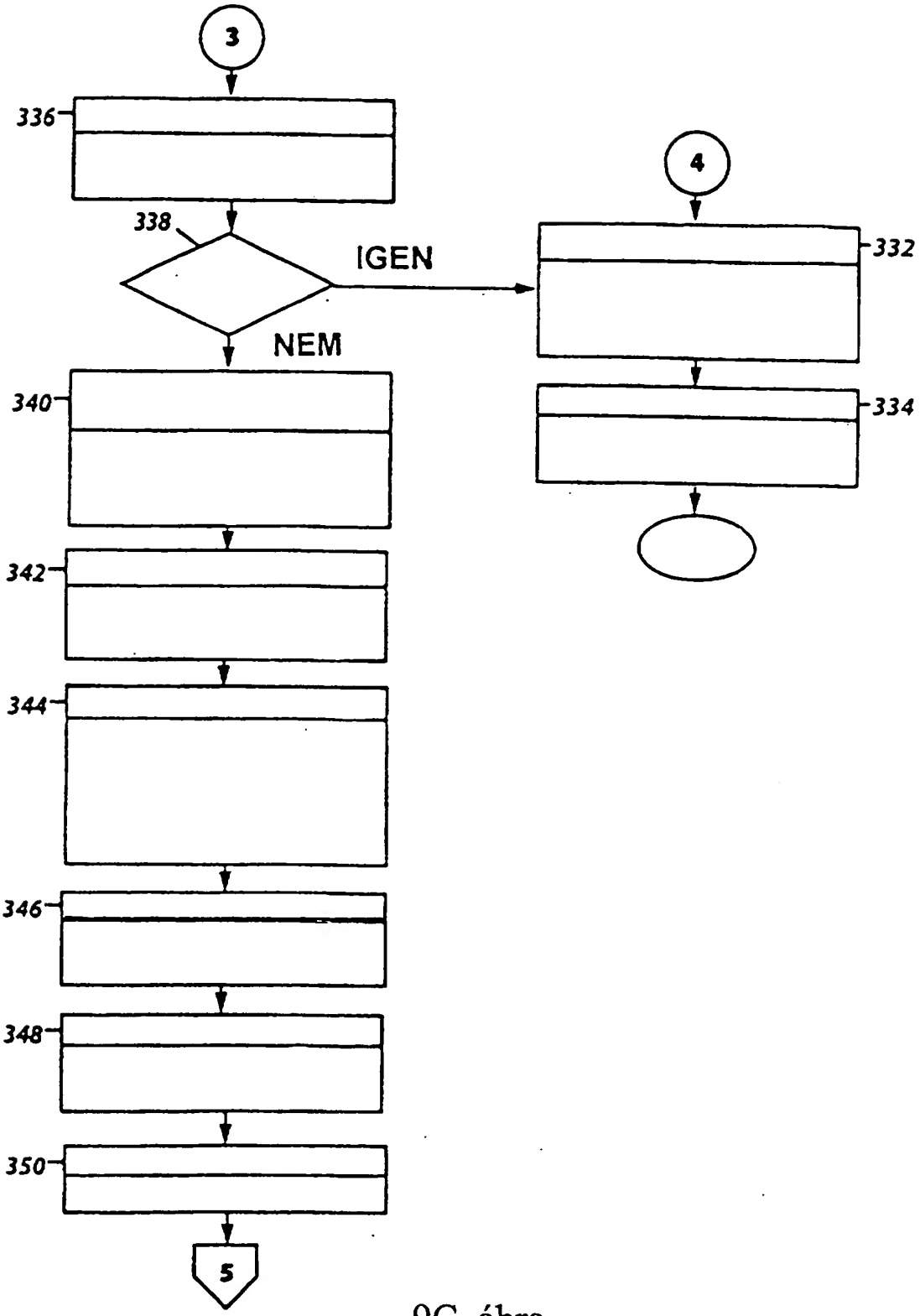
8D. ábra



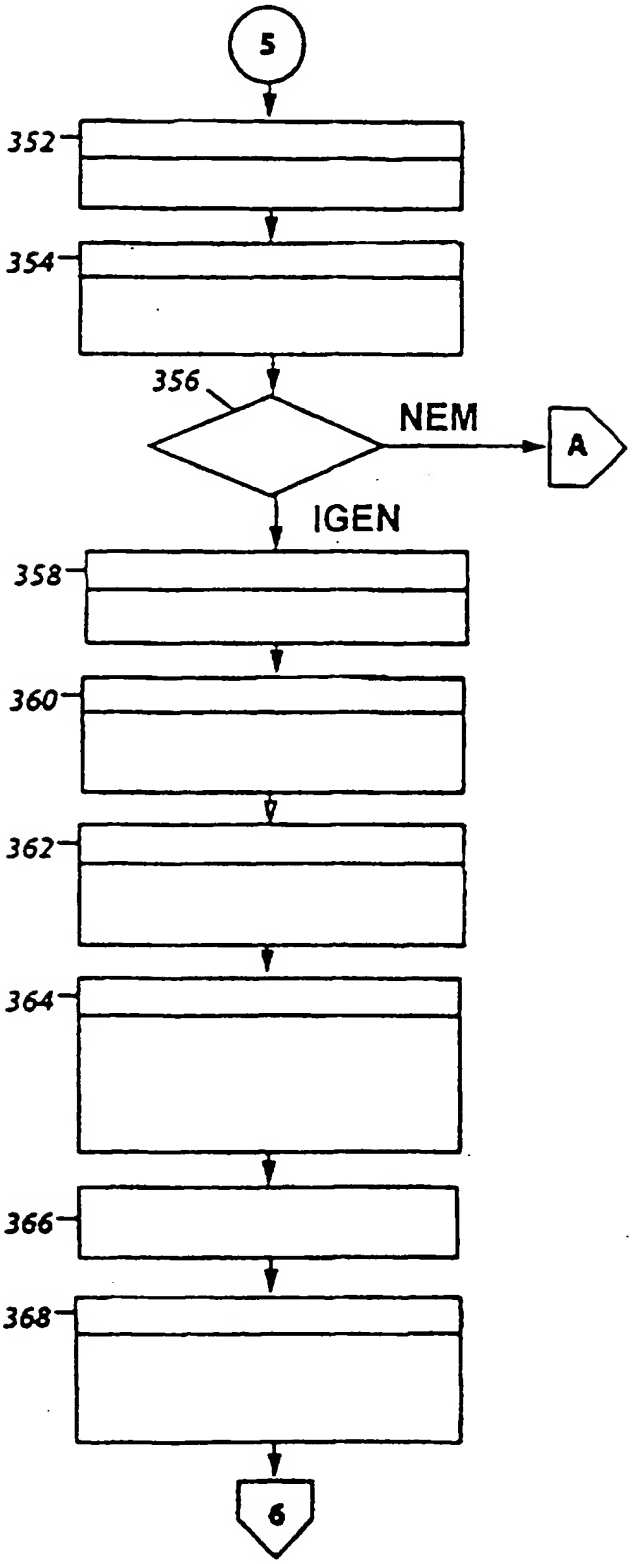
9A. ábra



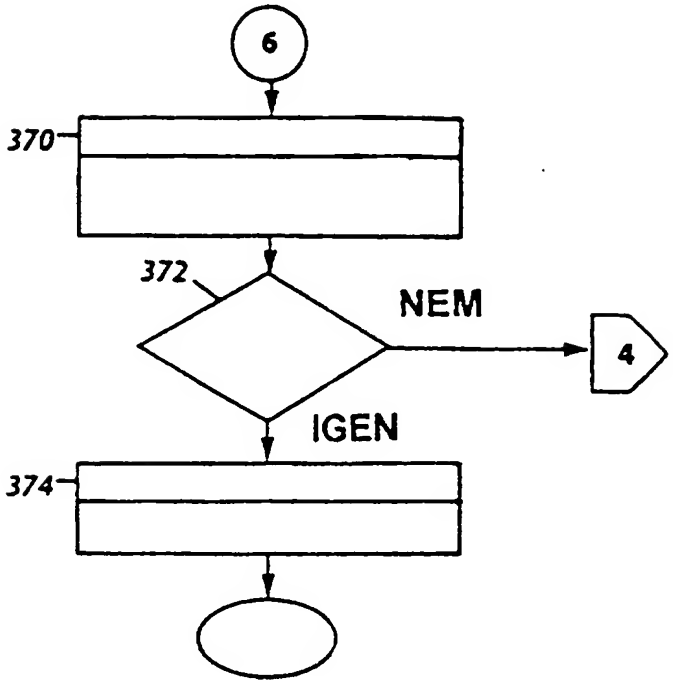
9B. ábra



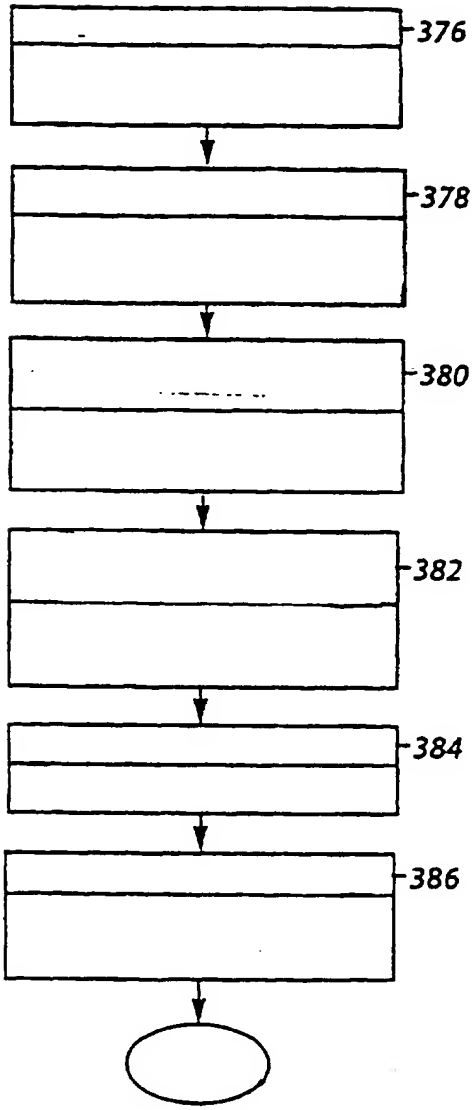
9C. ábra



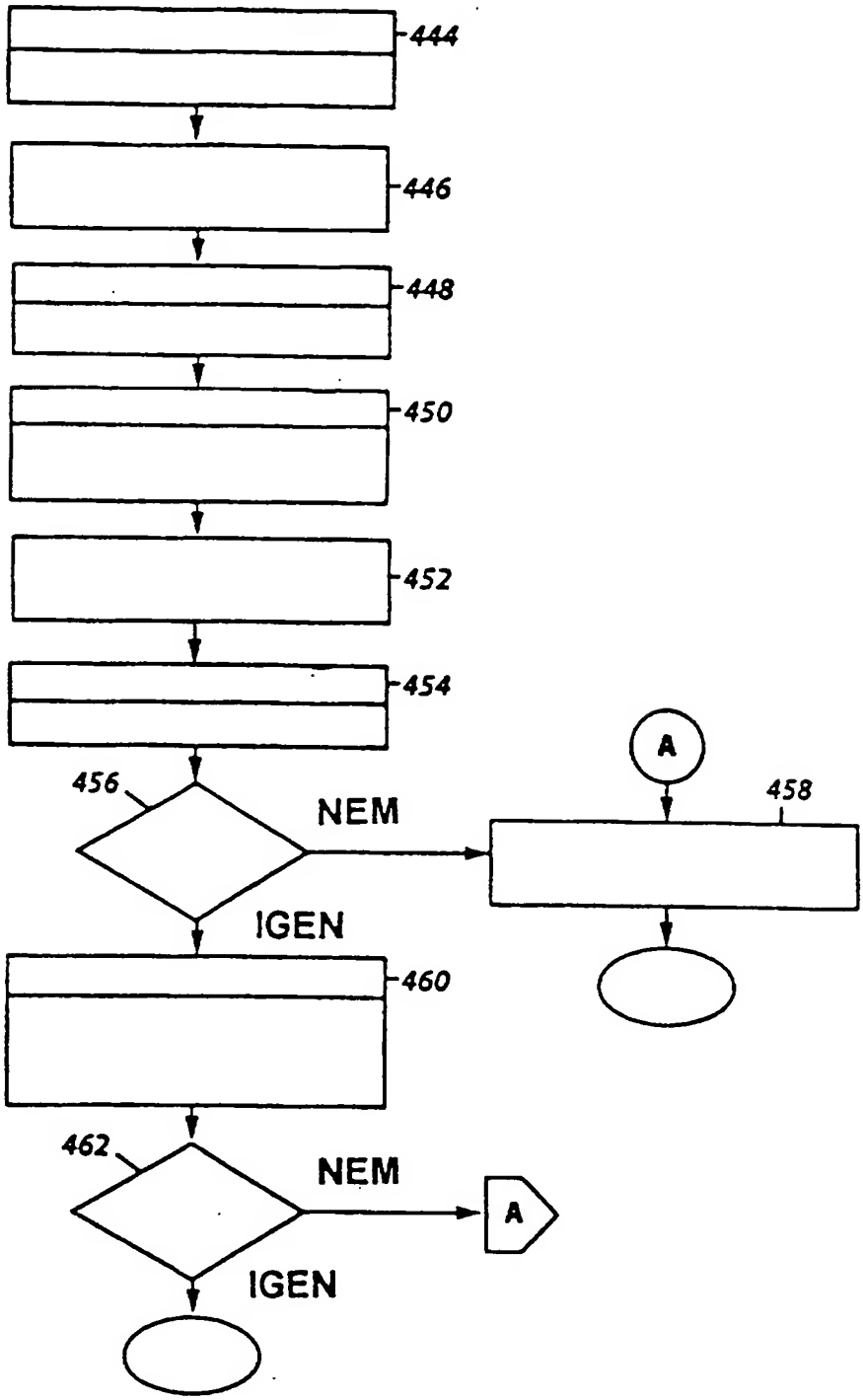
9D. ábra



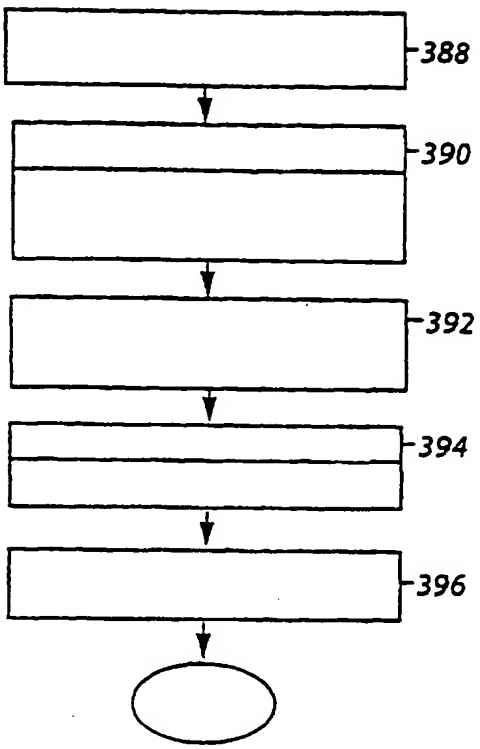
9E. ábra



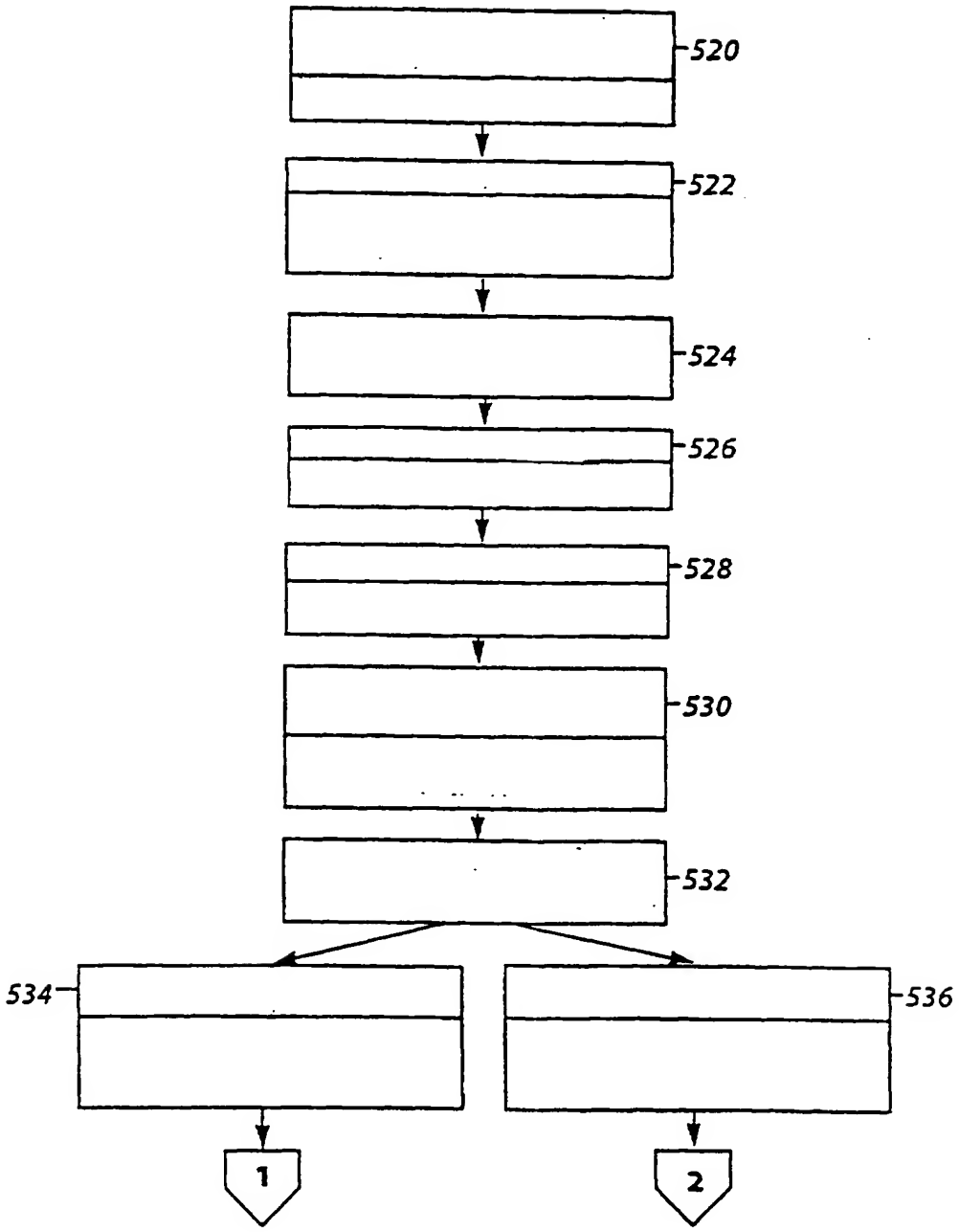
10. ábra



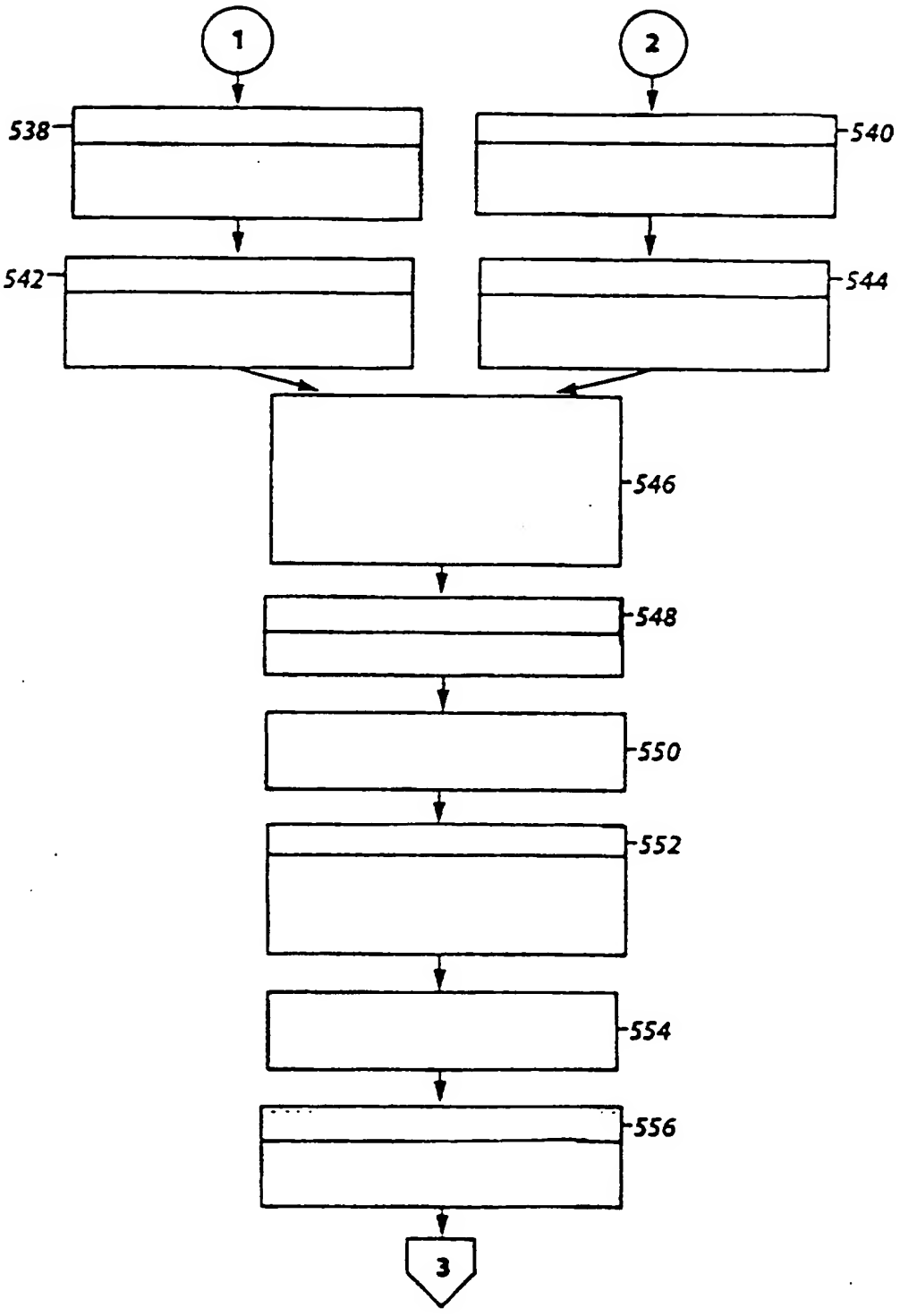
11. ábra



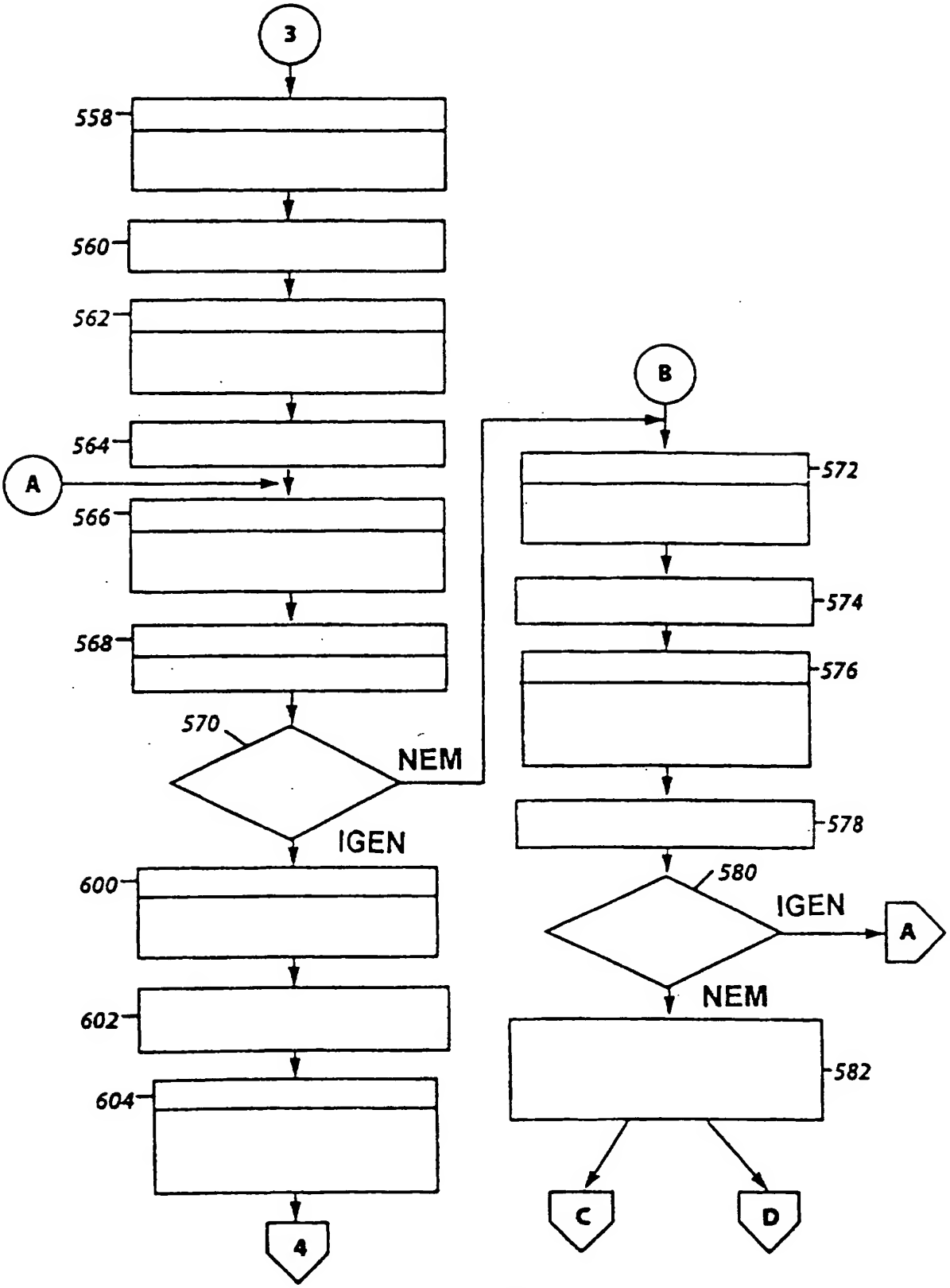
12. ábra



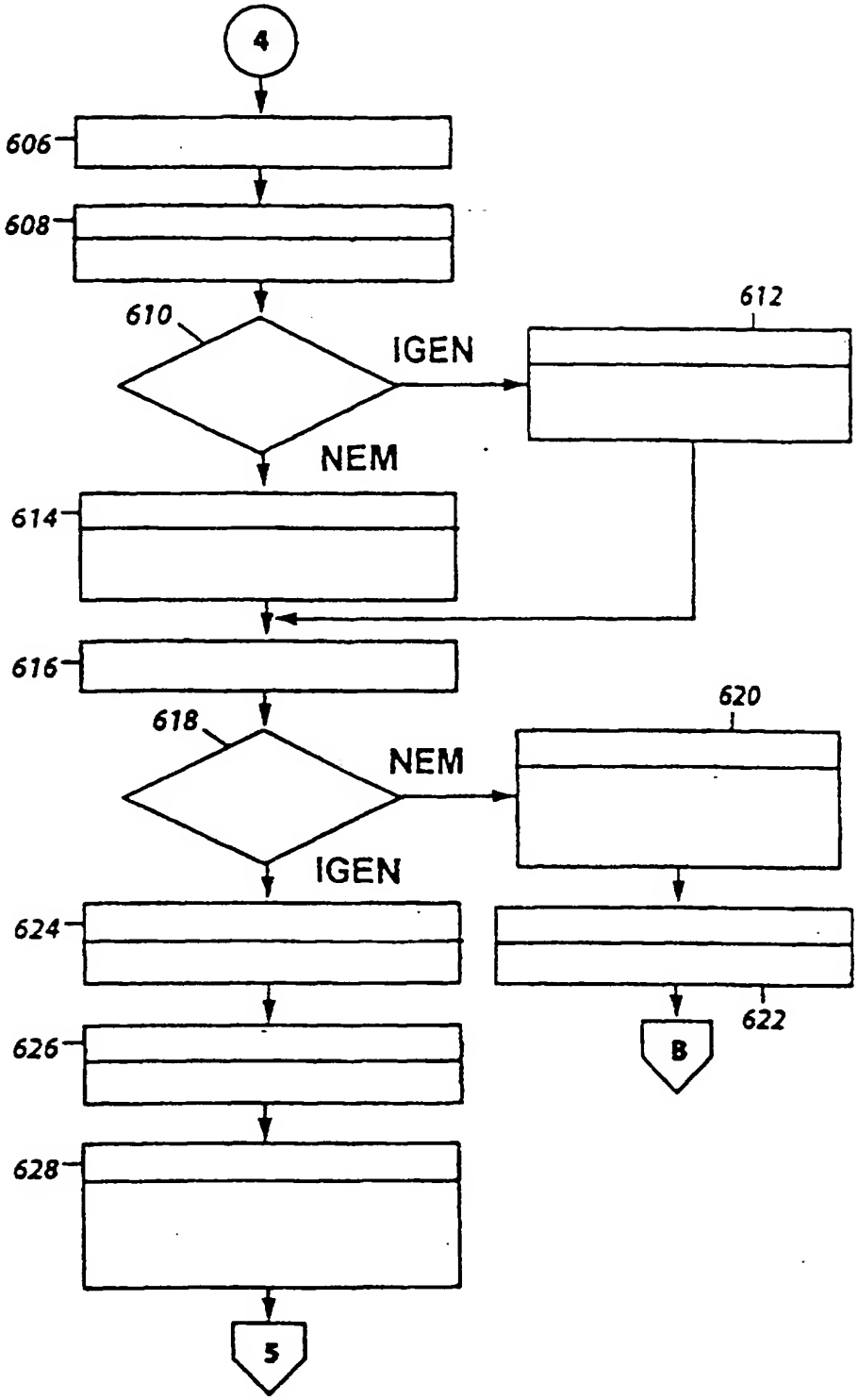
13A. ábra



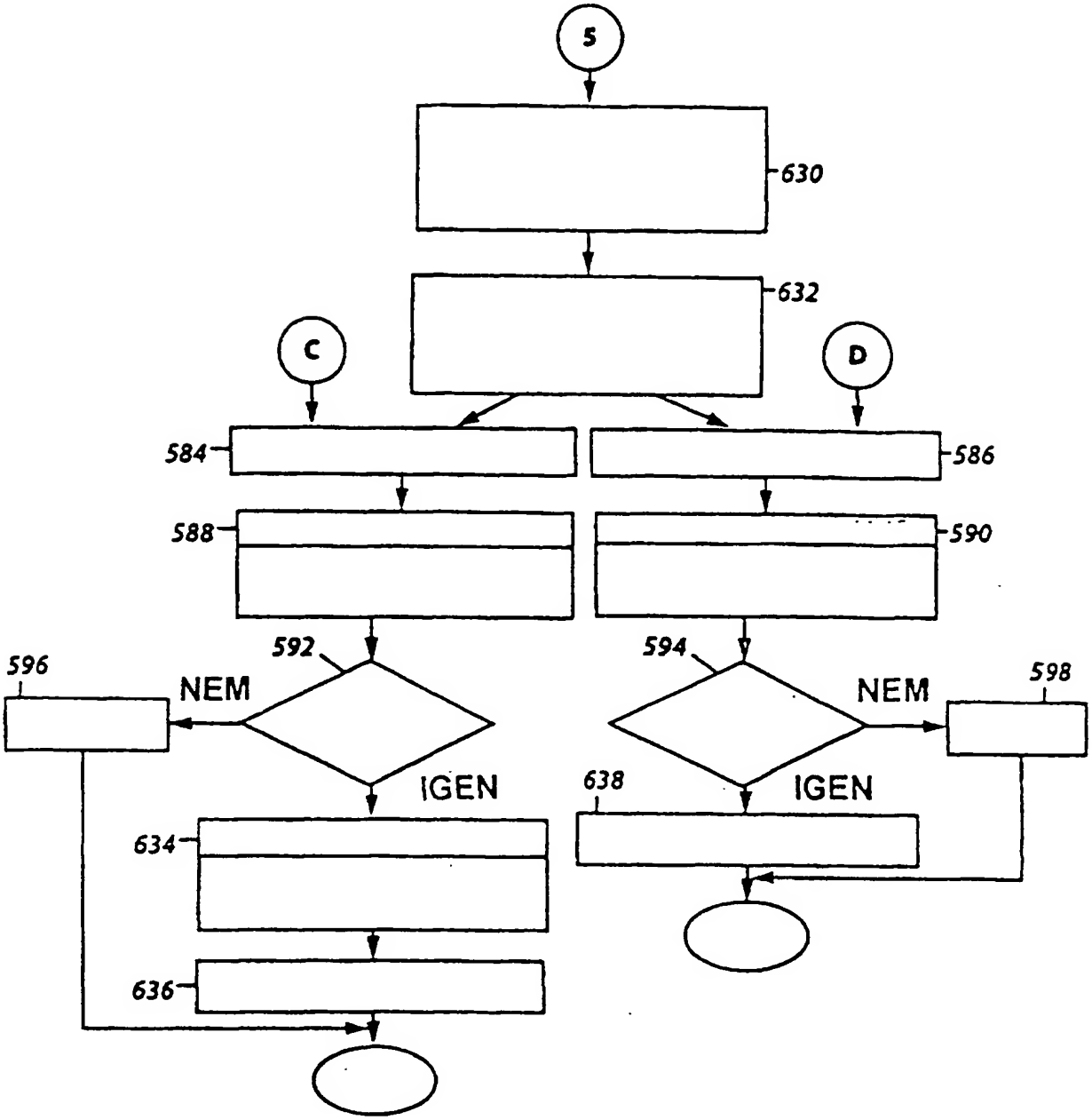
13B. ábra


3
558
560
562
564
A
566
568
570
NEM
IGEN
600
602
604
4
B
572
574
576
578
580
IGEN
A
NEM
582
C
D

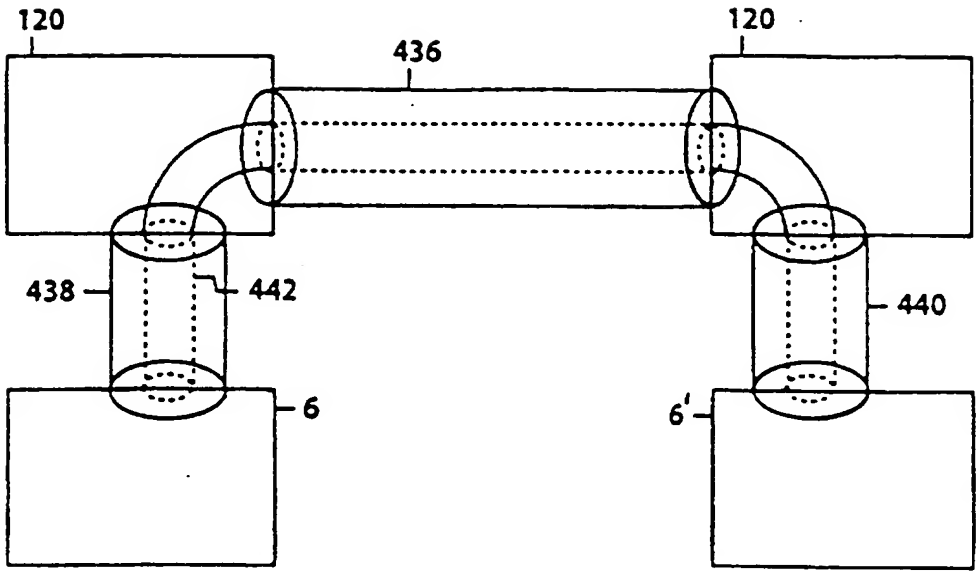
13C. ábra


4
606
608
610
IGEN
612
NEM
614
616
618
620
NEM
IGEN
624
626
628
622
B
5

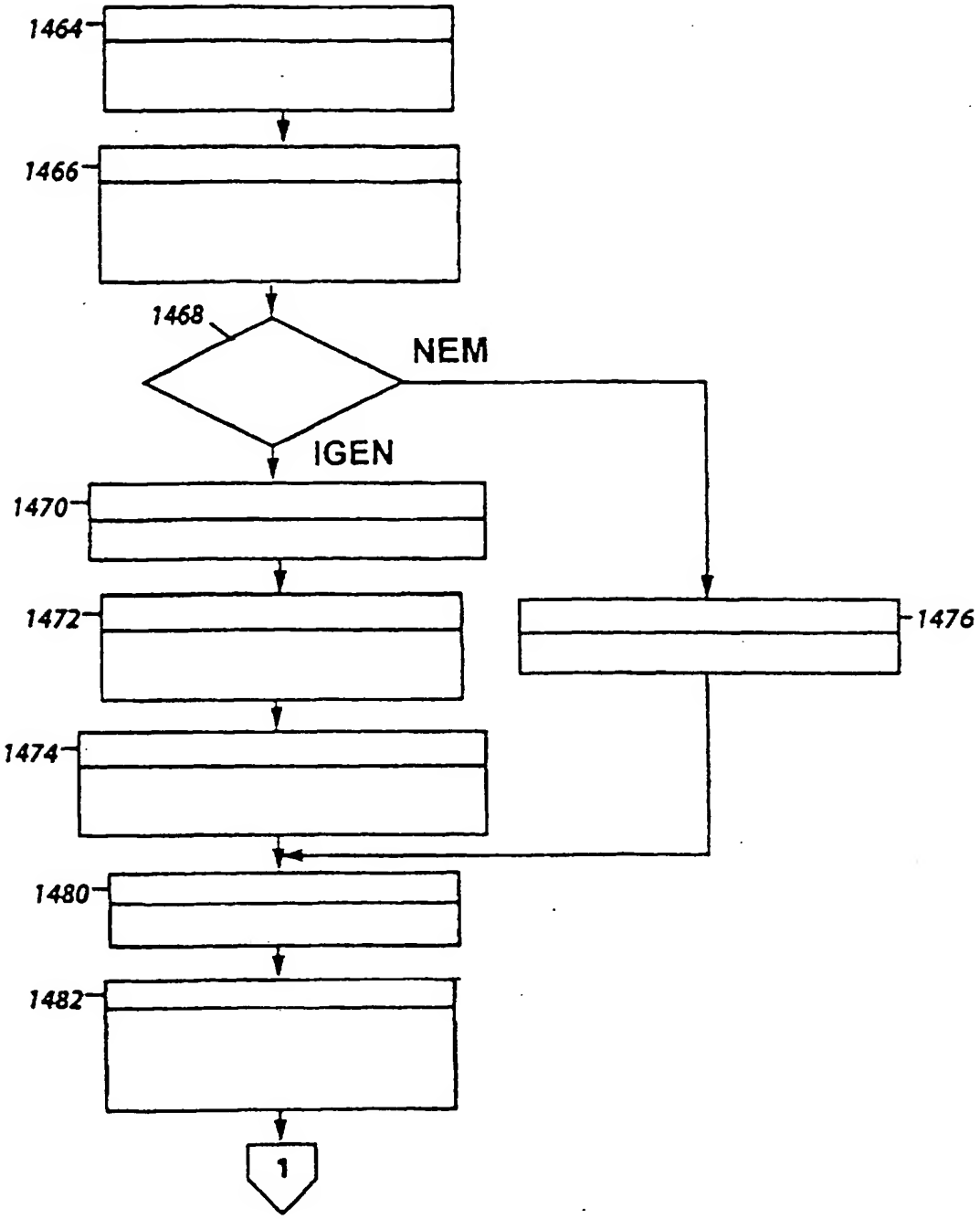
13D. ábra


5
630
632
C
D
584
586
588
590
592
594
596
NEM
IGEN
NEM
598
638
IGEN
634
636

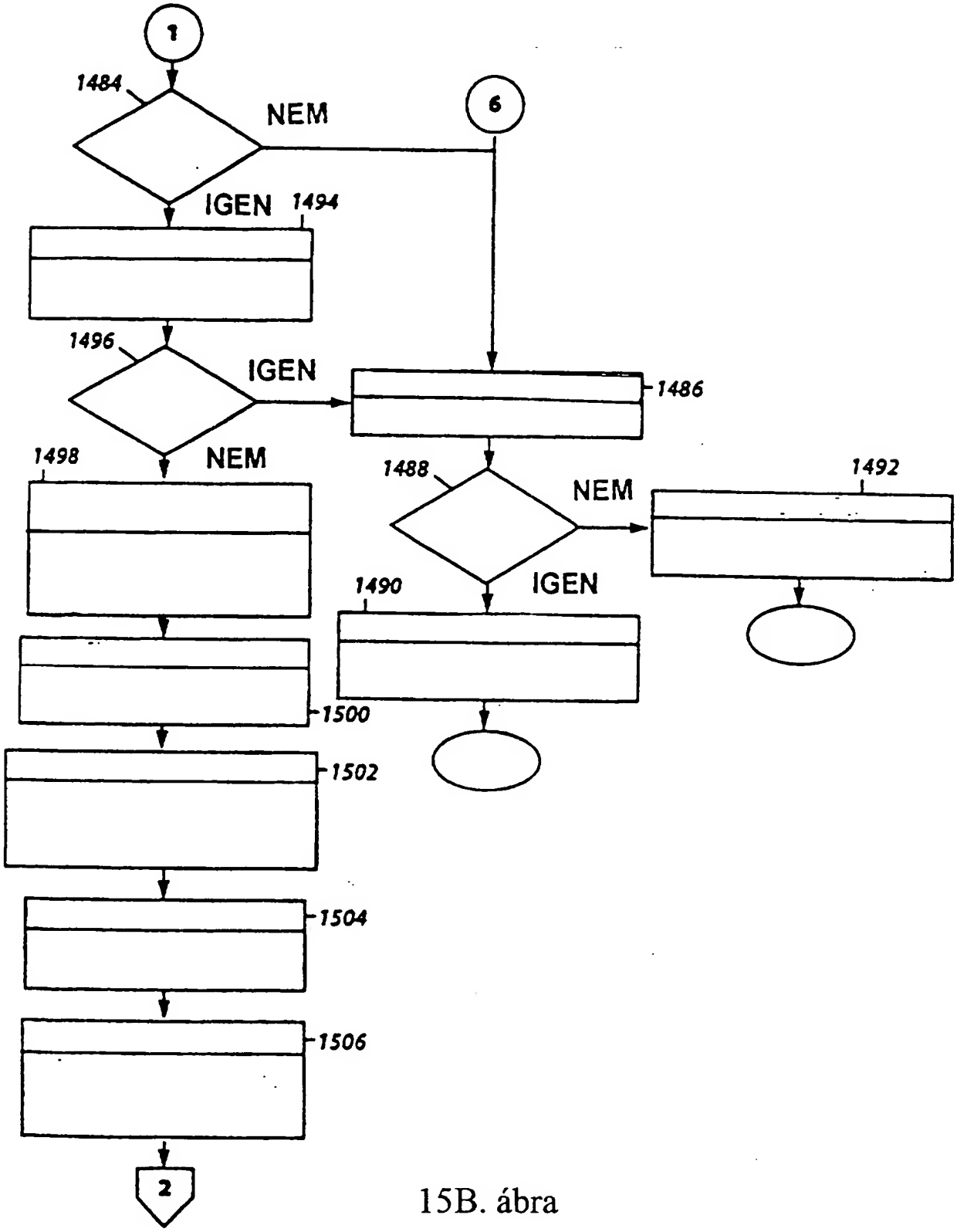
13E. ábra



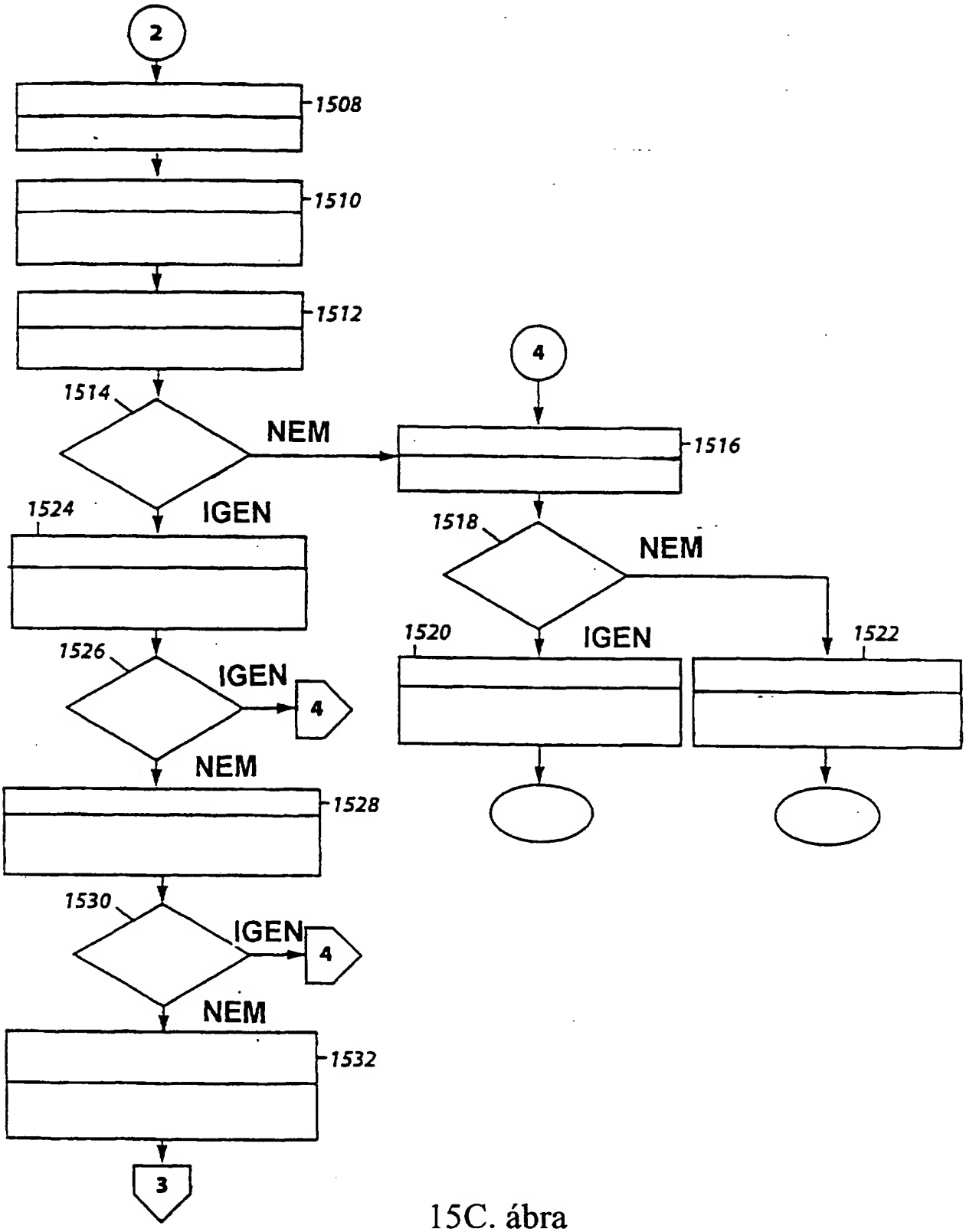
14. ábra



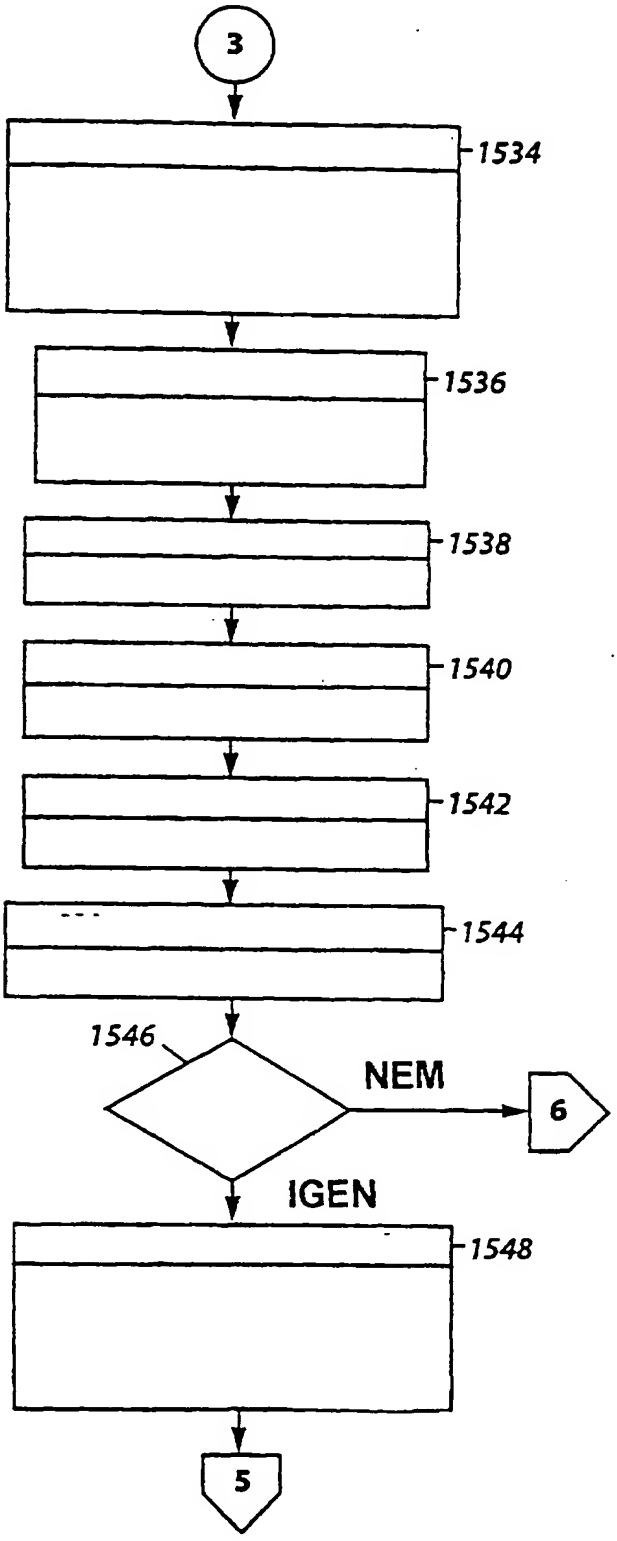
15A. ábra


1
1484
NEM
6
IGEN
1494
1496
IGEN
1486
1498
NEM
1488
NEM
1492
IGEN
1490
1500
1502
1504
1506
2

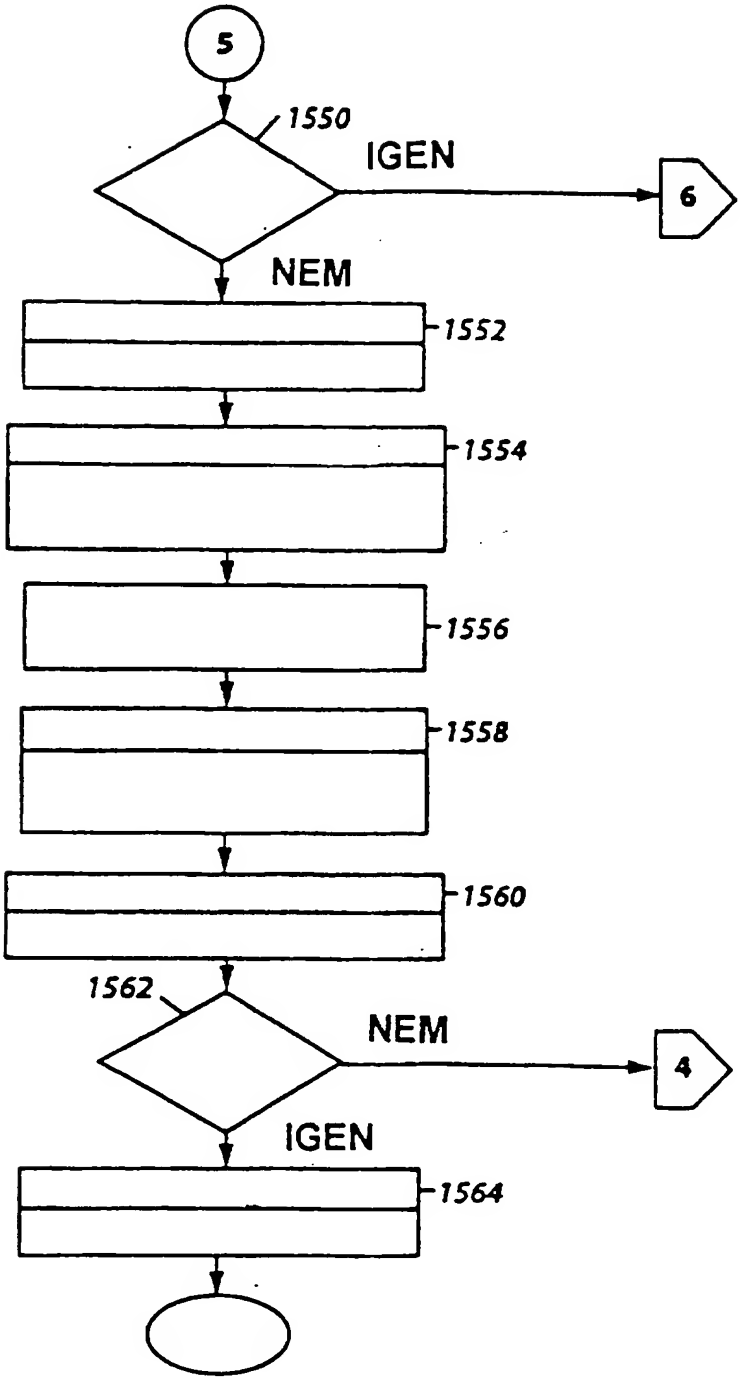
15B. ábra


2
1508
1510
1512
1514
NEM
4
1516
IGEN
1524
1518
NEM
1520
IGEN
1522
1526
IGEN
4
NEM
1528
1530
IGEN
4
NEM
1532
3

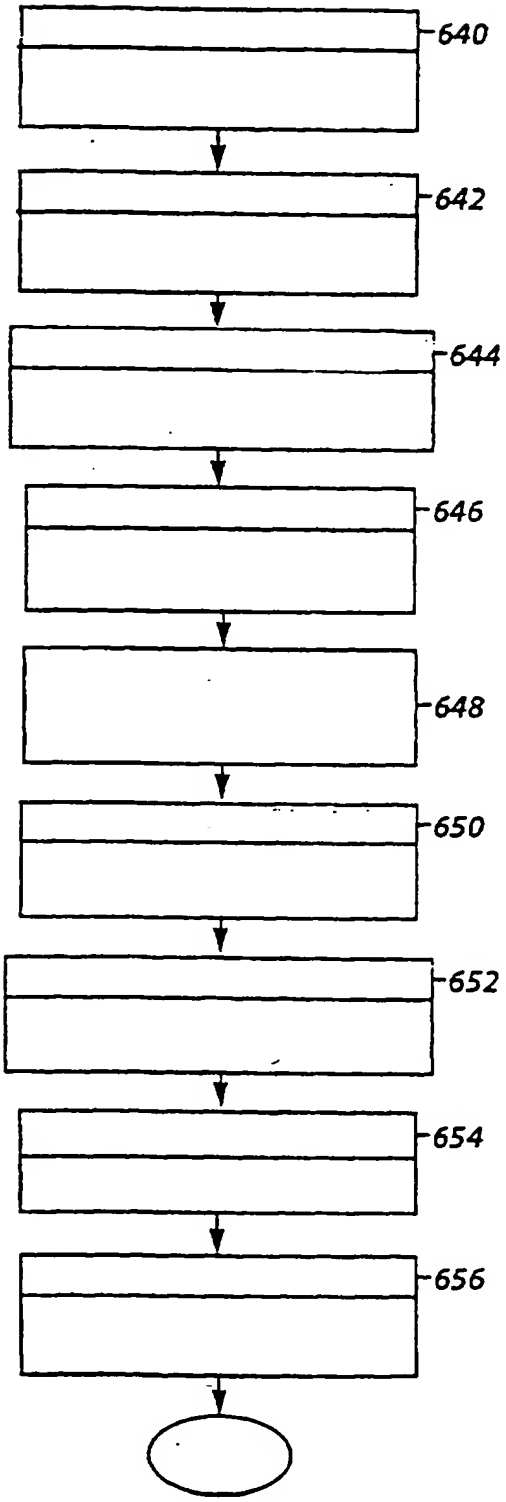
15C. ábra



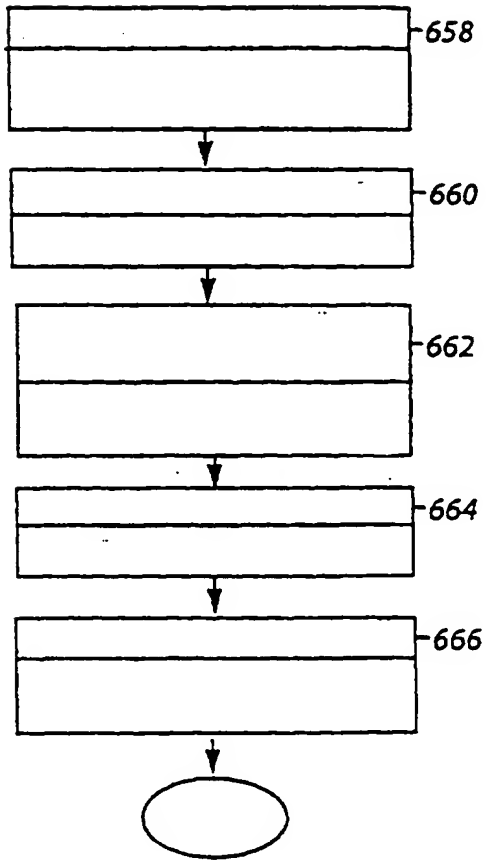
15D. ábra



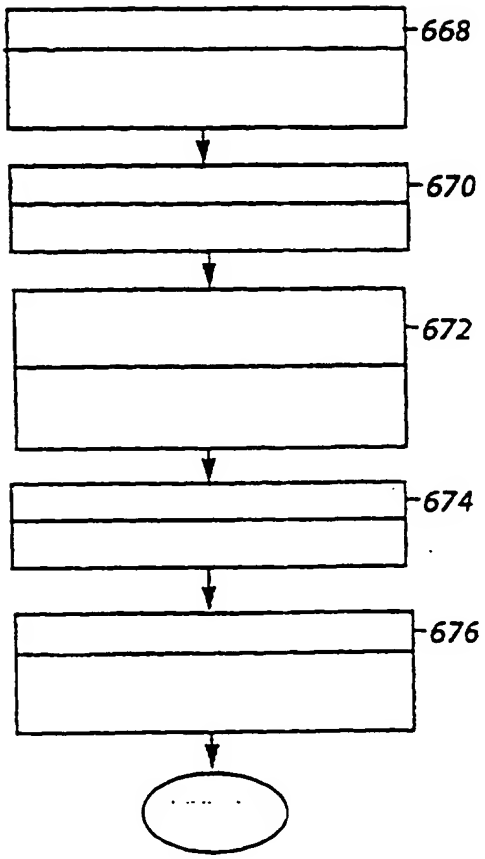
15E. ábra



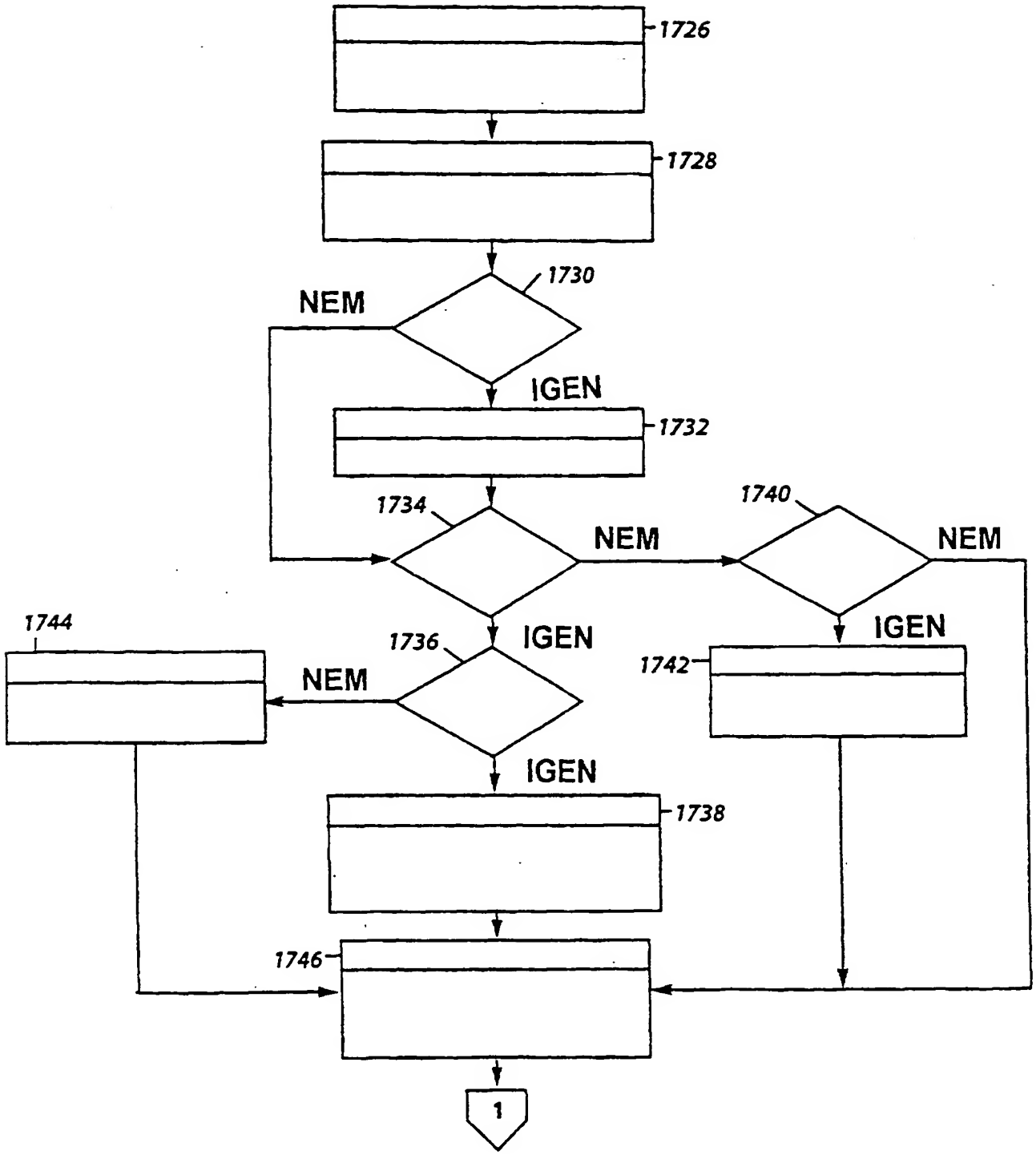
16. ábra



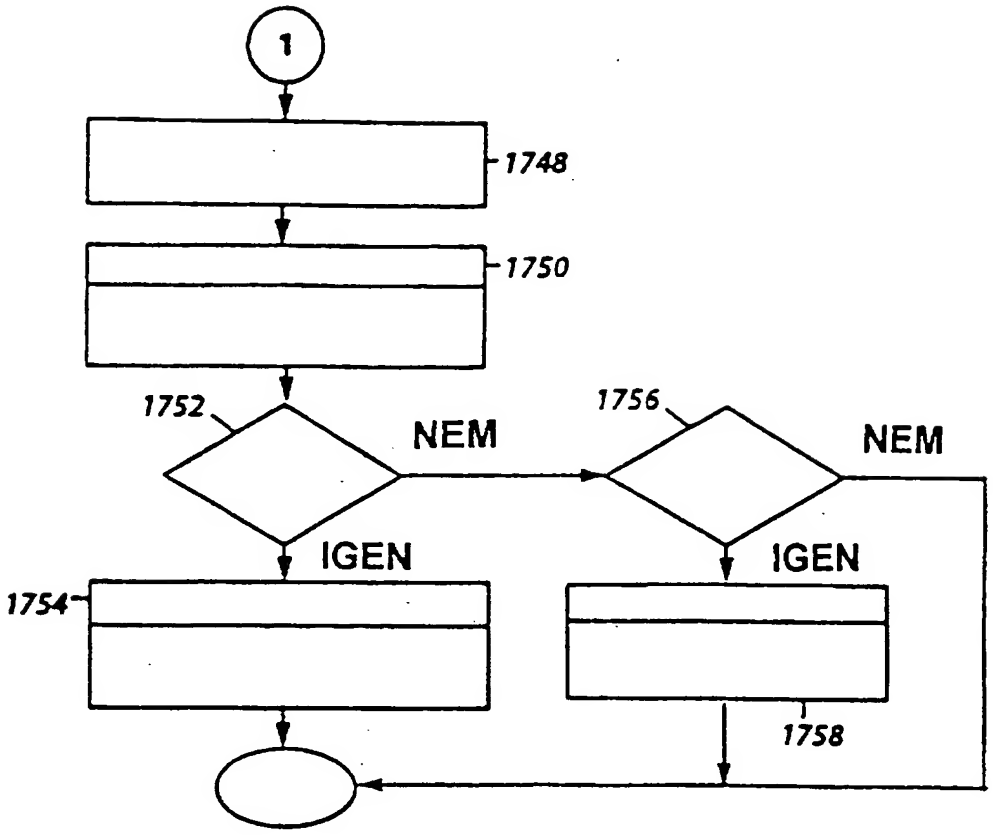
17. ábra



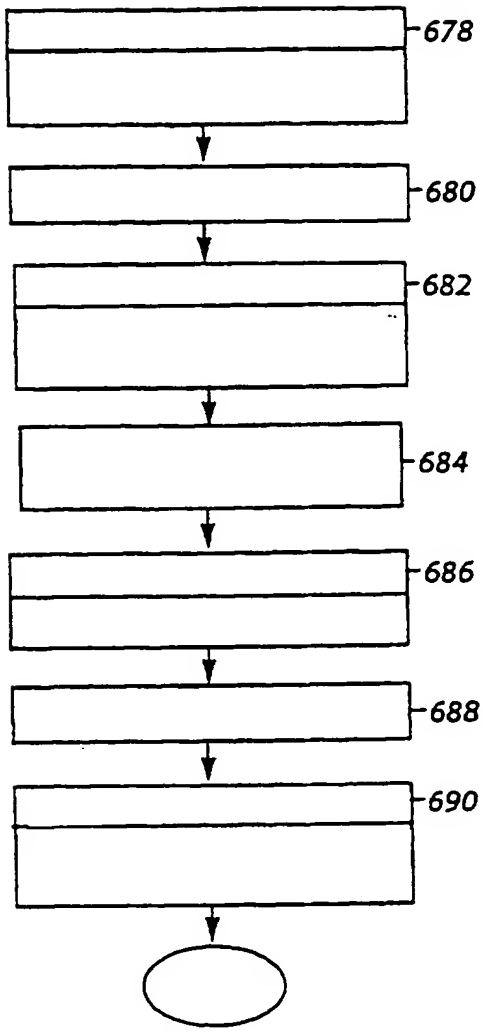
18. ábra


1726
1728
1730
NEM
IGEN
1732
1734
NEM
1740
NEM
1744
1736
IGEN
IGEN
1742
NEM
IGEN
1738
1746
1

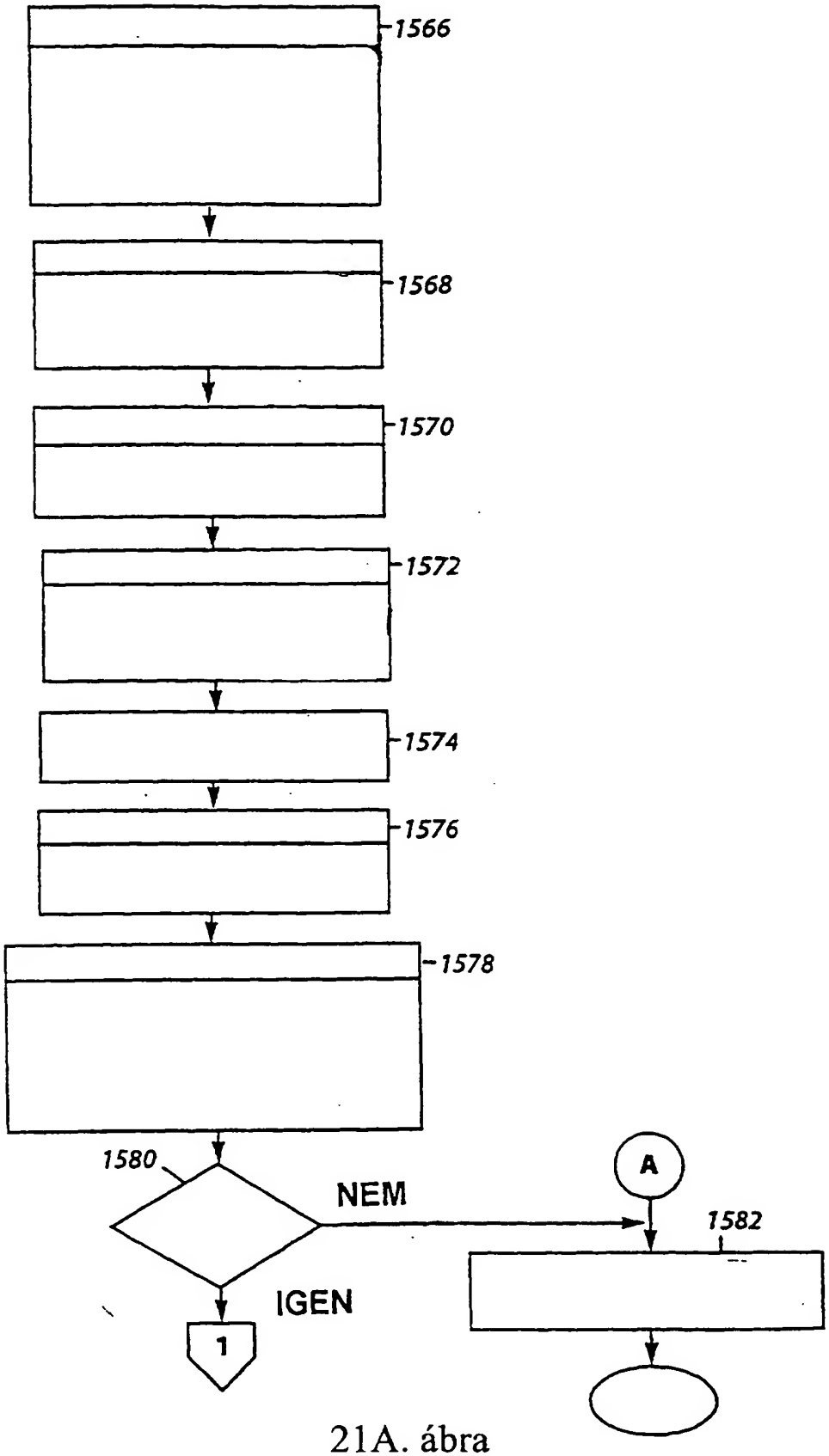
19A. ábra



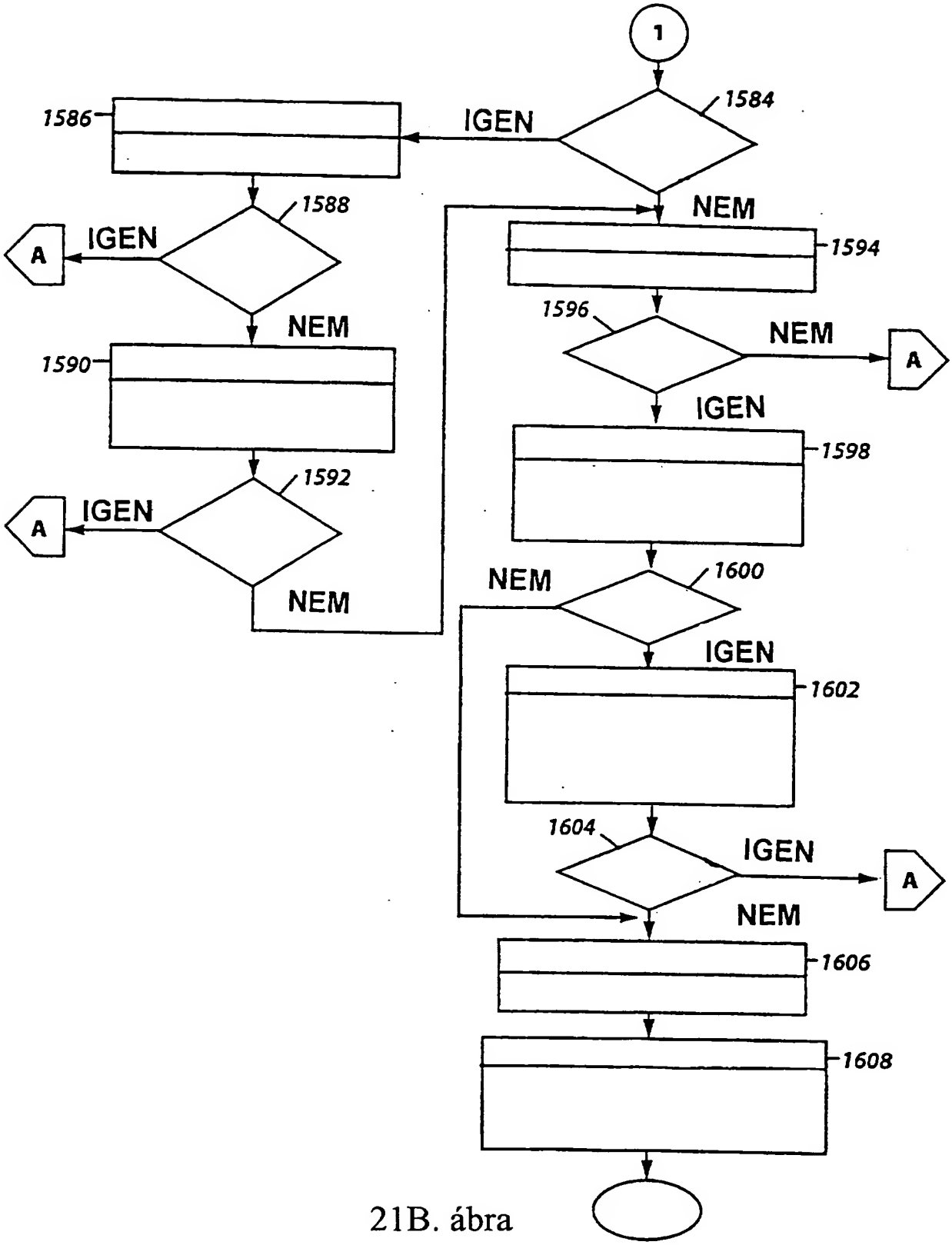
19B. ábra



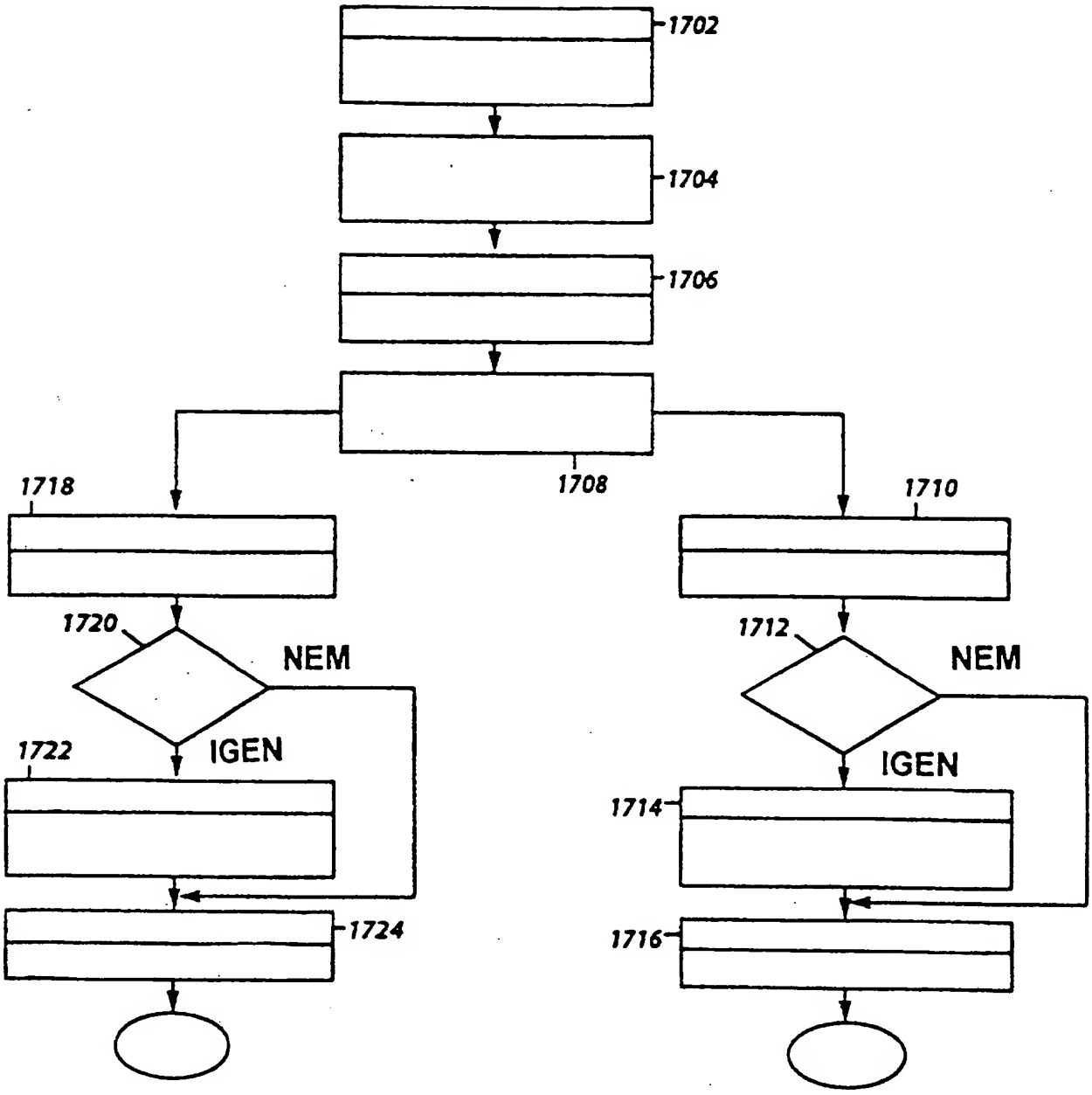
20. ábra



21A. ábra


1
1584
IGEN
1586
NEM
1588
A
IGEN
1594
NEM
1596
NEM
A
1590
IGEN
1598
1592
A
IGEN
NEM
1600
NEM
IGEN
1602
1604
IGEN
A
NEM
1606
1608

21B. ábra


1702
1704
1706
1708
1718
1710
1720
NEM
IGEN
1712
NEM
IGEN
1722
1714
1724
1716

22. ábra